

**SECURING CYBERSPACE: EFFORTS TO PROTECT
NATIONAL INFORMATION INFRASTRUCTURES
CONTINUE TO FACE CHALLENGES**

HEARING

BEFORE THE

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, AND INTERNATIONAL
SECURITY SUBCOMMITTEE

OF THE

COMMITTEE ON
HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

JULY 19, 2005

Printed for the use of the Committee on Homeland Security
and Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

23–163 PDF

WASHINGTON : 2006

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

SUSAN M. COLLINS, Maine, *Chairman*

TED STEVENS, Alaska	JOSEPH I. LIEBERMAN, Connecticut
GEORGE V. VOINOVICH, Ohio	CARL LEVIN, Michigan
NORM COLEMAN, Minnesota	DANIEL K. AKAKA, Hawaii
TOM COBURN, Oklahoma	THOMAS R. CARPER, Delaware
LINCOLN D. CHAFEE, Rhode Island	MARK DAYTON, Minnesota
ROBERT F. BENNETT, Utah	FRANK LAUTENBERG, New Jersey
PETE V. DOMENICI, New Mexico	MARK PRYOR, Arkansas
JOHN W. WARNER, Virginia	

MICHAEL D. BOPP, *Staff Director and Chief Counsel*

JOYCE A. RECHTSCHAFFEN, *Minority Staff Director and Chief Counsel*

TRINA D. TYRER, *Chief Clerk*

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, AND
INTERNATIONAL SECURITY SUBCOMMITTEE

TOM COBURN, Oklahoma, *Chairman*

TED STEVENS, Alaska	THOMAS CARPER, Delaware
GEORGE V. VOINOVICH, Ohio	CARL LEVIN, Michigan
LINCOLN D. CHAFEE, Rhode Island	DANIEL K. AKAKA, Hawaii
ROBERT F. BENNETT, Utah	MARK DAYTON, Minnesota
PETE V. DOMENICI, New Mexico	FRANK LAUTENBERG, New Jersey
JOHN W. WARNER, Virginia	MARK PRYOR, Arkansas

KATY FRENCH, *Staff Director*

SEAN DAVIS, *Legislative Assistant*

SHEILA MURPHY, *Minority Staff Director*

JOHN KILVINGTON, *Minority Deputy Staff Director*

LIZ SCRANTON, *Chief Clerk*

CONTENTS

Opening statements:	Page
Senator Coburn	1
Senator Carper	3
Senator Akaka	5
Senator Collins (ex officio)	6

WITNESSES

TUESDAY, JULY 19, 2005

Donald (Andy) Purdy, Jr., Acting Director, National Cyber security Division, Information Analysis and Infrastructure Protection Directorate, U.S. De- partment of Homeland Security	6
David A. Powner, Director, Information Technology Management Issues, U.S. Government Accountability Office	8
Paul M. Skare, Product Manager, Siemens Power Transmission and Distribu- tion, Inc., Energy Management and Automation	22
Thomas M. Jarrett, Secretary and Chief Information Officer, Department of Technology and Information, State of Delaware	25

ALPHABETICAL LIST OF WITNESSES

Jarrett, Thomas S.:	
Testimony	25
Prepared statement with attachments	105
Powner, David A.:	
Testimony	8
Prepared statement	46
Purdy, Donald (Andy) Jr.:	
Testimony	6
Prepared statement	35
Skare, Paul M.:	
Testimony	22
Prepared statement with attachments	69

APPENDIX

Questions and responses for the Record from:	
Mr. Purdy	120
Mr. Powner	153
Mr. Skare	158
Mr. Jarrett	164

**SECURING CYBERSPACE: EFFORTS TO
PROTECT NATIONAL INFORMATION
INFRASTRUCTURES CONTINUE TO
FACE CHALLENGES**

TUESDAY, JULY 19, 2005

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION, AND INTERNATIONAL SECURITY,
OF THE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:05 p.m., in room 562, Dirksen Senate Office Building, Hon. Tom Coburn, Chairman of the Subcommittee, presiding.

Present: Senators Coburn, Carper, Akaka, and Collins (ex officio).

OPENING STATEMENT OF CHAIRMAN COBURN

Senator COBURN. The Committee will come to order. This is the first of probably many hearings on cyber security within the Federal Government and I am going to have a very limited opening statement. Being from Oklahoma, we had some significant events there while I was a Member of Congress that taught us all a huge lesson in terms of terrorism. But there are several significant points associated with cyber security in America.

First of all, the United States does not currently have a robust ability to detect a coordinated cyber attack on our critical infrastructure, nor does it have a measurable recovery and reconstitution plan for key mechanisms of the Internet and telecommunications system.

Second, the Department of Homeland Security has not completed the National Infrastructure Protection Plan.

Third, cyber attacks on control systems can be targeted from remote locations around the globe. We know that.

Fourth, DHS is responsible for protecting the Nation's critical infrastructures. However, 85 percent of all the critical infrastructures are controlled by the private sector.

And then, finally, there is a lack of stable leadership at the National Cyber Security Division, which has hurt its ability to maintain trusted relationships with the private sector and has hindered its ability to adequately plan and execute activities.

This is the first of the hearings that we intend to hold to look at Internet and informational, as well as cyber security within this Subcommittee.

[The prepared statement of Senator Coburn follows:]

PREPARED STATEMENT OF SENATOR COBURN

On the morning of April 19, 1995, Oklahoma learned firsthand the horrific effects of terrorism in the homeland. The prevention of terrorism starts with a proactive plan with cogent, measurable goals and the development and empowerment of effective moral leaders to accomplish these goals.

In October 2003, Chairman Adam Putnam of the House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, held a hearing where he clearly identified the problem, saying, "The nation's health, wealth, and security rely on these systems, but, until recently, computer security for these systems has not been a major focus. As a result, these systems on which we rely so heavily are undeniably vulnerable to cyber attack or terrorism." Those vulnerabilities still exist today, only now they are less excusable. More importantly, the government's plan to secure our critical infrastructures from a cyber threat remains vague and formative despite clear legislative and executive mandates.

Since September 11, 2001, the focus of security in the United States has been on physical terrorist attacks. In contrast, the government's cyber security efforts have focused on the internet and networking and desktop functions we all use every day. Unfortunately, operational control systems, which are at the heart of our critical infrastructures, do not work like conventional desktop business computer systems. The President has spoken to this in Homeland Security Presidential Directive #7 (HSPD-7) and the National Strategy to Secure Cyberspace, emphasize that our nation's critical infrastructures provide services which are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

Congress has also spoken through The Homeland Security Act of 2002 which laid clear mandate on cyber security at Department of Homeland Security. The Act requires DHS to (1) assess our vulnerability to cyber attack (2) develop a plan to fix it and (3) implement that plan using measurable goals and milestones. In order to implement the plan the Department has the admittedly difficult task of engaging and securing action from diverse players, state and local governments, other federal agencies, especially key industry actors. Cyber vulnerability is primarily in the private sector and the Department must find a way to overcome the challenges there. The nature of terrorists is to attack private citizens as we recently saw in the horrific attack in the United Kingdom. There can be no excuse for not effectively engaging the private sector, even though it is hard. We ask no less of our food safety, airline security and pharmaceutical industries.

Nobody wants to micromanage the private sector; however, American expects DHS to take every reasonable measure to protect us from terrorism. I am not convinced that threshold has been met.

If America is to be safe from the damage of a cyber attack, we will need a plan, a budget tied to that plan and Congressional commitment to the implementation of the plan. In particular, I hope we can commit to the following:

1. The completion of the National Infrastructure Protection Plan, fully incorporating the cyber component with more than vague generalities;
2. A way to measure milestones in the NIPP that will be assigned to a named department head;
3. A budget line item associated with the milestones.

To that end, I look forward to hearing from our witnesses from GAO, DHS, the State of Delaware, and Siemens Power Transmission & Distribution, Inc.

Senator COBURN. At this time, I will yield for an opening statement to the——

Senator CARPER. Be careful what you say. [Laughter.]

Senator COBURN [continuing]. Ranking Member, and my friend, the other "TC" on the Subcommittee, for his opening statement. Senator Carper, thank you for being here.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Thank you, Mr. Chairman. I am happy to be here with you and Senator Collins and to welcome our first panel of witnesses and look forward to the next panel of witnesses, which includes an old friend from—not an old friend, but a good friend from Delaware, one of our leaders.

I would just reflect back. I think some 2 weeks ago now, we had the devastating terrorist attacks on the London transportation system and it reminded us once again—especially those of us who live in the Northeastern corridor of the United States—it reminded us once again that terrorists are increasingly able to exploit our vulnerabilities and to cause an enormous amount of damage, destruction of property and taking of human lives.

Since September 11, the majority of our Homeland Security efforts have been aimed to strengthen security of our Nation's physical infrastructure. A good example of that is the aviation industry. Some of us are hopeful it eventually will focus more on rail and transit and subways, too.

Last week, the Homeland Security and Governmental Affairs Committee held under Senator Collins's leadership—I think it might have been in this room—held a hearing on protecting chemical facilities within the United States. The hearing highlighted the necessary precautionary measures that should be taken to protect a chemical facility from a terrorist attack.

The importance of cyber security is oftentimes overlooked in discussions involving homeland security. Cyber security, though, plays an important role in the protection of our critical infrastructures. Computers and networks provide an increasing convenience and effectiveness for the everyday operation of critical infrastructures. In fact, on a critical infrastructure such as a railroad, combined with a cyber attack on the computer system of a major electric utility, it can have an enormous impact on the emergency response capabilities that are needed in times of disaster.

It is the Committee's job, this Committee, and I think specifically this Subcommittee, it is our job to ensure that we are taking the steps that are needed to minimize the chance and to minimize the consequences of such an attack if it occurs.

Again, I mention, Mr. Chairman, we have one of my friends and colleagues from Delaware, Tom Jarrett, not a "TC" but a "TJ," who is our Chief of Information. He works in the Governor's cabinet, heads up the Department in our State called the Department of Information and Technology and I am just delighted to hear from Tom and to see him again.

Accompanying Secretary Jarrett, I am told, is a woman named Elayne Starkey, and I am looking out in the audience. I think she is sitting right behind—there she is. Elayne, welcome. When you see Tom Jarrett's lips move, hear his voice speak later on, you will see Elayne's lips move. When I was privileged to be Governor, she just did great work, helping us really to bring technology to bear in our law enforcement efforts and we will always be grateful for the great work that she did.

We are going to hear from Secretary Jarrett today about a Department of Technology Information that is really all too familiar with the challenges that are facing cyber security. One of Dela-

ware's critical infrastructures is our State computer network. It is a large target of over, listen to this, 3,000 cyber attacks per day, little Delaware. I can't imagine what happens in big States like yours, but over 3,000 cyber attacks per day. I am not sure why that is. Maybe it is because we are the home of incorporation of over half-a-million companies, half the New York Stock Exchange, half the Fortune 500. I am not sure what it is, but that is a lot of attacks.

Secretary Jarrett implemented a number of cyber security initiatives to address the cyber risks associated with our State's computer network. Delaware's Department of Technology and Information aims to strengthen and provide proper cyber security through partnerships with State agencies, multi-state forums, and a collaborative with Microsoft Corporation. Secretary Jarrett meets on a routine basis with all cyber security stakeholders to share cyber threat and vulnerability information to better protect our State's network from cyber attacks. Delaware's cyber security initiatives are an excellent example, we believe, of the processes and partnerships that are needed to protect against cyber attacks.

In May 2005, at the request of Senator Lieberman, our colleague, and several Representatives, including Chris Cox, Representative Davis, Representative Thornberry, Lofton, the Government Accountability Office released a report that was titled, "The Department of Homeland Security Faces Challenges in Fulfilling Cyber Security Responsibilities." That is a pretty big title. The report criticized the Department of Homeland Security's efforts thus far in fulfilling its cyber security responsibilities that are established for in law and policy.

To fulfill the Department's cyber security responsibilities, such as assessing national cyber threats and vulnerabilities, the Government Accountability Office recommends that the Department of Homeland Security improve organizational stability and foster better partnerships with the private security, much as we have done in Delaware.

As demonstrated by Delaware's Department of Technology Information, partnerships provide education, the technical expertise, and information sharing outlet that is needed to effectively secure cyber assets. Proper information sharing between the Federal Government and the private sector is instrumental to protecting our Nation's critical infrastructure from cyber attack.

Last week in this room, Secretary Chertoff laid out a reorganization plan of the Department that includes a new Assistant Secretary for Cyber Security and Telecommunications to strengthen information technology management and cyber security responsibilities within the Department of Homeland Security. As that Department sets forth in strengthening national cyber security initiatives and efforts, I ask that the Department build cyber security partnerships within the private sector and provide a road map of priorities and milestones of cyber security responsibilities and initiatives, much as we have done in our State and perhaps in your States, as well.

I really do look forward to this hearing and the testimony from all of our witnesses concerning the challenges that we face along these lines and the Federal Government's role, our role, in pro-

tecting our Nation's critical infrastructures from a cyber attack. I hope that the discussion that occurs here today and following this hearing will lead us to real solutions to the challenges that we face within the Federal Government with respect to cyber security.

Mr. Chairman, I thank you, and to our witnesses, welcome. We look forward to hearing from you. Thanks.

Senator COBURN. Senator Akaka, I understand that you have a hearing that you need to chair at 2:25. The Chairman has graciously allowed you to go ahead of her, if you would care to make your opening statement.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Chairman Coburn. Thank you for permitting me to do it now, and thank you, Chairman Collins, for letting me do this.

Chairman Coburn, I want to compliment you on holding today's hearing on cyberspace. I know we both are also interested in agroterrorism, so these are up and coming issues, and I thank you so much for giving me this time.

Computers and computer networks reside at the heart of the systems upon which the American people rely on on a daily basis. As our witnesses know, many of these systems are far too vulnerable to cyber attack, which would inhibit their function, corrupt important data, and expose private information.

The Internet is the backbone of the U.S. economy and our Nation's critical infrastructures. It is the electronic roadway of commerce, industry, and defense. Databases stored on computer networks, in particular, have been an attractive target for criminal hackers who have breached the networks of several well-known companies and have stolen the personal data of millions of Americans. A successful attack on the computer systems that support our critical infrastructures would threaten our national security, public health, and, of course, our way of life.

The former head of the National Infrastructure Protection Center, Ron Dick, once said, "The thing that keeps me awake at night is the thought of a physical attack on the U.S. infrastructure combined with a cyber attack which disrupts the ability of the first responders to access 911 systems." This is not an exaggerated fear, as our own military realizes the power of cyber warfare in destroying an enemy's command and control.

The Department of Homeland Security is responsible for protecting the key resources and critical infrastructures in the United States. In carrying out this role, DHS has a number of responsibilities established by law and Presidential directive. We are here today to discuss these DHS issues and how DHS is fulfilling those responsibilities and the specific challenges that the Department faces as it moves forward.

One area that is of particular concern to me is the failure by DHS to complete a comprehensive cyber threat and vulnerability assessment. This threat assessment should be the foundation for the Department's risk-based approach to mission and priorities. A comprehensive threat assessment is needed in order to be certain that we are adequately protected and to ensure that precious Federal dollars are well spent.

I want to thank you, Mr. Chairman, for having this hearing today and thank you for the time and wish you well. We look forward to our witnesses' testimony. Thank you.

Senator COBURN. Thank you, Senator Akaka.

Now, I am pleased to recognize the Chairman of the full Committee, Susan Collins from Maine. Thank you, Senator.

OPENING STATEMENT OF CHAIRMAN COLLINS

Chairman COLLINS. Thank you very much. Let me begin by thanking you, Mr. Chairman, for convening this hearing today and shining a spotlight on a critical infrastructure issue.

And your timing could not be better. Just last week, Secretary Chertoff testified before the full Committee regarding his Second Stage Review recommendations for the Department of Homeland Security. As Senator Carper has mentioned, Secretary Chertoff proposes to create a new Assistant Secretary for Cyber Security and Telecommunications, a position that has long been needed.

Clearly, Secretary Chertoff has acknowledged that cyber security is an issue worthy of much more attention and resources from within the Department. This hearing will provide an opportunity to explore some of the challenges that the new Assistant Secretary will face.

Computers and information systems are key components that support the operations of critical infrastructure in our country, whether it is chemical facilities or oil refineries, dams, power systems, telecommunications, or mass transit systems. Increasing computer interconnectivity has improved the quality of daily life for Americans, but unfortunately, this interconnectivity has also created a weakness that can be exploited by our enemies in this post-September 11 world.

I am pleased that the Department is placing more emphasis on this vital component of our Nation's critical infrastructure sectors and I look forward to working with you, Mr. Chairman, as well as the Department to strengthen our protections and defenses in this area.

Senator COBURN. Thank you, Madam Chairman.

Our first panel consists of two witnesses, Andy Purdy, Acting Director, National Cyber Security Division of the Department of Homeland Security, and David Powner, Director of IT Management at GAO.

Mr. Purdy, your complete statement will be made a part of the record. If you would limit your comments to 5 minutes, I would appreciate it. Thank you.

TESTIMONY OF DONALD (ANDY) PURDY, JR.,¹ ACTING DIRECTOR, NATIONAL CYBER SECURITY DIVISION, INFORMATION ANALYSIS AND INFRASTRUCTURE PROTECTION DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. PURDY. Thank you. Good afternoon, Chairman Coburn and Madam Chairman Collins. My name is Andy Purdy. I am the Acting Director of the National Cyber Security Division (NCSA) within the Department of Homeland Security. I am delighted to appear

¹The prepared statement of Mr. Purdy appears in the Appendix on page 35.

before you today on behalf of my colleagues to share with you the work of NCSA and those with whom we are partnering.

In today's world, we recognize that attacks against us may manifest in many forms, including physical and cyber. We recognize the potential impact of collateral damage from any one attack to a variety of assets. As such, our Directorate takes a holistic view of critical infrastructure vulnerabilities and works to protect America from all threats by ensuring the integration of physical and cyber approaches.

NCSA was created in June 2003 to serve as a national focal point for cyber security and to coordinate the implementation of the national strategy to secure cyberspace. Our mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.

To meet that mission, we have developed a set of goals with specific objectives for each goal and milestones, and we have identified two overarching priorities. One, to build a national cyberspace response system. Two, to implement a cyber risk management program for critical infrastructure protection. Focusing on these two priorities establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

A core component of our effort to establish a national cyberspace response system is the US-CERT Operations Center, a partnership between DHS and the public and private sectors. US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our Nation's cyber infrastructure.

To assist Federal agencies in protecting their cyber infrastructure, we have established the Government Forum of Incident Response and Security Teams to facilitate interagency information sharing and cooperation across Federal agencies for readiness and response efforts.

A key component of our response system is the Cyber Annex, which we created as part of the recently issued National Response Plan, that provides a framework for responding to cyber incidents. To provide a Federal approach to coordinated cyber incident response, we worked with the Departments of Defense and the Departments of Justice to form the National Cyber Response Coordination Group, later formalized by the Cyber Annex as the principal Federal interagency mechanism to coordinate preparation for and response to cyber incidents of national significance.

Under our second priority, we are engaged in a risk management program to assess threats and reduce the risk to our critical infrastructure. For the cyber component of the National Infrastructure Protection Plan, DHS is the sector specific agency, with our Division as the lead for the information technology sector, and we are working with the IT ISAC and the newly formed Information Technology Sector Coordinating Council to identify critical assets, assess vulnerabilities, and determine protective measures.

In addition, we are attempting to ensure that cyber is comprehensive throughout this national plan by providing guidance to the other critical infrastructure sectors in analyzing, identifying, and assessing and protecting their cyber assets and the cyber com-

ponent of their physical assets. Within this framework, we are pursuing other priority vulnerability reduction effort: The Internet Disruption Working Group, our Control Systems Security Program, and our Software Assurance Program.

We believe the recent GAO report on critical infrastructure has provided a fair assessment of the progress to date and we agree that while considerable work has been done, much work remains to meet the challenges in this rapidly changing area. With the proposed appointment of a new Assistant Secretary for Cyber and Telecommunications Security, we are confident that we will accelerate our cyber security efforts.

Secretary Chertoff's recent release of the findings from his second stage review of the entire Department illustrates DHS's commitment to addressing leadership and organizational concerns that also have been raised by GAO. We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts at the State and Federal level, and academia to formulate the partnerships and leverage the efforts of all, including the private sector, so that we as a Nation are more secure in cyberspace.

Again, thank you for the opportunity to testify before you today and I would be glad to answer any of your questions.

Senator COBURN. Thank you very much, Mr. Purdy. Mr. Powner.

TESTIMONY OF DAVID A. POWNER,¹ DIRECTOR, INFORMATION TECHNOLOGY MANAGEMENT ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. POWNER. Dr. Coburn, Chairman Collins, and Ranking Member Carper, we appreciate the opportunity to testify on the Department of Homeland Security's efforts associated with securing our Nation's infrastructures from cyber security threats.

Recent attacks and threats have underscored the need to effectively manage and bolster the cyber security of our Nation's critical infrastructures. For example, criminal groups, foreign intelligence services, and terrorists are threats to our Nation's computers and networks. Regarding recent attacks in March of this year, hackers gained access to the electric industry's control systems.

To address these threats, Federal law and policy calls for critical infrastructure protection activities and establishes DHS as our Nation's focal point. It also designates other agencies to coordinate with key sectors, including energy, banking and finance, transportation, and telecommunications.

This afternoon, I will summarize four points, as requested. First, DHS has many responsibilities called for in law and policy. Second, although progress has been made in each area, much work remains ahead. Third, DHS faces many challenges in fulfilling these responsibilities. And fourth, Several recommendations remain outstanding that, if effectively prioritized and addressed, could greatly improve our Nation's cyber security posture.

Expanding on each of these, first, we recently reported that based on Federal law and policy, DHS's 13 key cyber security re-

¹ The prepared statement of Mr. Powner appears in the Appendix on page 46.

sponsibilities that include developing a national plan, enhancing public and private information sharing of cyber threats, vulnerabilities, and attacks, conducting a National Threat Assessment, facilitating vulnerability assessments, and coordinating incident response and recovery efforts if, in fact, an attack occurs. Although DHS has initiated efforts that begin to address each of these 13 responsibilities, the extent of progress varies and more work remains on each.

For example, its Computer Emergency Response Team, referred to as the US-CERT, issues warnings on vulnerabilities and coordinates responses to cyber attacks. However, our Nation still lacks a National Threat Assessment, sector vulnerability assessments, a mature analysis and warning capability, and key recovery plans, including plans for recovering the Internet.

DHS faces many challenges in building its credibility as a stable, authoritative, and capable organization that can fulfill its cyber critical infrastructure responsibilities. These include achieving organizational stability and authority. Over the past year, multiple DHS cyber security executives have left the Department. Establishing the Assistant Secretary for Cyber may help. However, leveraging this new authority and recruiting top talent to fill it remains a challenge.

Another challenge is establishing effective partnerships and information sharing arrangements with other government entities and the private sector. During our most recent review, representatives from the banking and finance sector told us that the level of trust is not sufficient to have productive information sharing.

In addition, DHS needs to demonstrate value, meaning that it needs to provide useful and timely information on such items as threats and analytical products to key stakeholders.

Over the last several years, we have made a series of recommendations to enhance the cyber security of critical infrastructure that demand immediate attention, including conducting important threat and vulnerability assessments, developing a strategic analysis and warning capability to identify potential attacks, developing a strategy to protect infrastructure control systems, and developing recovery plans to respond to attacks. We also recommended that DHS prioritize its critical activities and closely monitor progress with appropriate performance measures.

In summary, Mr. Chairman, DHS has made progress in planning, in coordinating efforts to enhance cyber security, but much more needs to be done, including conducting threat and vulnerability assessments, bolstering our cyber analytical capabilities, aggressively pursuing threat and vulnerability reduction efforts, and developing recovery plans.

Our testimony today lays out a comprehensive road map for what remains to be accomplished in each area. Until DHS addresses its many challenges and more fully completes critical activities, it cannot function as the cyber security focal point intended in Federal law and policy, resulting in increased risk that large portions of our national infrastructure are unprepared to effectively manage cyber security attacks.

This concludes my statement. I would be pleased to respond to any questions you have at this time.

Senator COBURN. Thank you, Mr. Powner.

I have numerous questions. I will not ask them all at the hearing, but I would like for each of you to agree to answer in written form the questions that we will submit for the record and do that on a fairly timely basis, if you would not mind. That will spare you some time.

Mr. Purdy, when is it anticipated that the National Infrastructure Protection Plan will be completed?

Mr. PURDY. Well, Acting Under Secretary Robert Stefan has told the Hill that he expects to have a version of the plan in pretty good order by the end of the summer, so we don't have a precise date on that.

Senator COBURN. Will the reorganization, the stage two review, move that later?

Mr. PURDY. Oh, I don't expect so. No, sir.

Senator COBURN. If you don't care to comment on this, it is fine, but will this protection plan be beefed up with milestones that are linked to the budget line items and the department heads that are carrying that out?

Mr. PURDY. I am not sure that the plan that is in existence at the end of the summer will have that, but that is anticipated to be part of the plan as it rolls forward, including the specific sector plans that have to be developed in partnership between the government and the private sector, yes.

Senator COBURN. It seems that some industry sectors are more mature with regards to securing their cyber assets than others. I think that is a true statement. That is probably true throughout the residential cyber areas, as well. It seems that the title of the new Assistant Secretary for Cyber Security and Telecommunications would indicate that some critical infrastructures have more security needs than others, like the electric, chemical, telecommunication industries. Which sectors are more technologically mature and could be used as examples for sectors that are less mature when building guidance with which to self-regulate?

Mr. PURDY. Well, until we do a complete assessment by sector, it is difficult to give a quantitative approach to that. I certainly believe that the telecommunications and finance sectors are among the most robust.

Senator COBURN. We did have the penetration of some of the power companies' data. It kind of scares you when "24" is doing this ahead of the cyber crooks. As this NIPP plan comes up, one of the questions I think a lot of people are wondering, why is it taking so long to do that? Why is it taking so long to have a National Infrastructure Protection Plan?

Mr. PURDY. Well, I think it is a very difficult task. But on some of the specific items you mentioned, we have accelerated the prioritization of three major areas that we believe, although part of the National Infrastructure Protection Plan framework, deserve accelerated efforts. Those are our Internet Disruption Working Group that we co-chair with National Communication Systems, and Department of Treasury and others are members of that. So that is a high-priority effort, to identify the assets, the interdependencies, the protective measures, the response and the recovery, building on the ESF-II, which as you know has evolved from tele-

communications to communications generally. So that piece of it is fairly robust and that group will work to accelerate that and respond to some of the specific areas in the GAO report.

In addition, our control systems effort is a very robust effort that we brought over from our Protective Security Division in May 2004. We had the strategic plan. We had our goals. We have a tremendous partnership with the Department of Energy, with the Idaho National Lab and other labs.

And finally, our Software Assurance Program is also very robust, building on a key partnership with the Department of Defense, co-founding the National Infrastructure—the NIAP review in terms of the acquisition piece.

So we think those three priority efforts are not being held up by any time frame of the National Infrastructure Protection Plan and we believe those are the priorities, and so they are very important to us.

Senator COBURN. So your testimony is, sometime after the first of the year, we ought to have this plan intact, the NIPP plan?

Mr. PURDY. Actually, if I said that, I didn't mean to say that.

Senator COBURN. You said, by the end of this summer, we are going to have the structure of it, is that right?

Mr. PURDY. We are going to have a plan that is in pretty good shape. It is not going to be the final draft of it, yes.

Senator COBURN. But sometime after the first of the year, we should be able to expect that moving forward? I know you are implementing sections of that even before you have the NIPP plan, but for cyber security, where are we within that?

Mr. PURDY. Well, cyber security, we are moving forward in the work with the emerging Sector Coordinating Council, as you know, the private sector group, and the Government Coordinating Council. In fact, I think the organizations of one of your witnesses, NASCIO is a member of the Government Coordinating Council of the IT sector. And so we are working to build the framework for the sector-specific plan and the cyber guidance that will go to all the critical infrastructures. So that is moving ahead, and I certainly expect that the cyber piece will be ready well before the first of the year.

Senator COBURN. Now, you have an Internet Disruption Working Group.

Mr. PURDY. Yes.

Senator COBURN. Would you mind providing the Subcommittee a list of the achievements of that group, where you started and where you are now? One of the things that Mr. Powner said that really bothers me is that some of the limitation is because there is a lack of a level of trust. Those were his words just a moment ago. Do you perceive that is real? Is it founded on real actions? In other words, do they perceive a threatened loss of some technologic advance or proprietary information by working with you as we try to do this?

Mr. PURDY. Well, I think we are moving ahead very successfully in trying to facilitate information sharing with the private sector. As you may know, our secure portal, our US-CERT portal that involves approximately 200,000 government and private sector folks, we are working to integrate into the Homeland Security Informa-

tion Network. In addition, we are very excited by our partnership with the IT ISAC and the eight other ISACs that supply them cyber information so that we can incorporate that flow among those nine ISACs with the government into the HSIN structure.

In addition, the private sector is standing up an information sharing group and we will be sending some members to it to try to facilitate the exchange of value and incorporation of private sector input into the articulation of a threat. So the information can be shared among groups and move out in a way that efficiently gets to folks in a timely fashion. So we think that is very substantial progress.

In addition, we are reaching out to the private sector to convene some meetings that will be in the early fall to bring in the incident response teams from major private sector entities from across the country to engage in training and moving forward to really target the information sharing, building on the existing information sharing of US-CERT and the efforts in information sharing from the ISACs that I just mentioned.

Senator COBURN. Are those web portals that you mentioned 100 percent secure?

Mr. PURDY. Well, we believe they are secure. I am not sure that there is a standard in current technology to say that something is 100 percent secure.

Senator CARPER. I want to back up if we could just a little bit and take a somewhat different approach. I don't care who leads off, but talk to us about the nature of the threat that we face. Talk to us about where the threat is coming from. Talk with us about whether the threat is rising, and if so, in what respect.

And you have touched on this a little bit, Mr. Purdy, but I mentioned in my remarks about our folks that were here from Delaware who will testify shortly, how we partner with the private sector, and I just want to hear your thoughts about those kinds of partnerships.

Mr. PURDY. The cyber assessment of threat was completed in the form of the National Intelligence Estimate for Cyber that we partnered with the intelligence and the law enforcement community on. Subsequent to that—and there are classified and unclassified versions of the NIE for cyber—subsequent to that, we have worked through our Information Analysis Division to provide intelligence collection requirements to the intelligence community for cyber, and those include information that would provide indicators of attacks against critical infrastructure, including control systems.

Senator CARPER. What kind of control systems are we talking about?

Mr. PURDY. Across the critical infrastructure.

Senator CARPER. Just give me some examples.

Mr. PURDY. Well, we have them in power, in chemical, in water. There are some in telecommunications. There are some in the finance industry. Most of the critical infrastructure sectors, pipelines, have control systems, and that is why it is one of the major priorities in our effort and in our funding.

Senator CARPER. Is it fair to say that those different critical infrastructures are under attack on a daily basis, weekly basis, monthly basis, or some never under attack?

And if so, where are the attacks coming from? What is the source of those attacks?

Mr. PURDY. The National Intelligence Estimate for Cyber identified some particular Nation States that are the source of particular kinds of attacks. There are attacks that are rampant throughout cyberspace. Within minutes, as you probably know, when you hook up a new computer, you can see different levels of attack. Obviously, we are more focused, particularly focused on attacks against major critical infrastructure, attacks, whether successful or otherwise, targeted against control systems, for example, and that is a major effort for us.

Working with the Process Control System Forum, hundreds of private sector owners and operators that we are partnering with with DOE to try to make sure we build access to the information and provide protective guidance, such as we issued last week, Control Systems Information Bulletin for guidance to the control systems owners and operators to help raise the bar in terms of those efforts.

A lot of the activity, the malicious activity in cyberspace right now, as you know, is targeted toward financial gain. The use and exploitation of vulnerabilities, the use of trojans and worms, there was an ABC news report last night on the use of keystroke loggers, the malicious code put on people's computers that log the personal identifying information, much of which is related to phishing and spam and identity theft. It is a major problem to our e-commerce in general, our financial community in particular, even though I think they are one of the most robust sectors in terms of financial security.

And so we are working with Treasury. We met with the FBIC, that is the governmental group, 2 weeks ago to try to accelerate the information sharing in the financial sector, and we are also monitoring the black market in those malicious tools, because there is a black market in those tools.

We are concerned and trying to help raise the bar because of the potential ability to use those vulnerabilities, to use those exploits to launch targeted, sophisticated attacks against our critical infrastructure, and that is why one of the priorities that I reference in my written testimony is trying to engage more effectively with the private sector on the priority areas that we need to focus on, and the one that we are suggesting to them is the identification of the major cyber attack scenarios, the serious cyber attack scenarios that we need to identify so we can mitigate, prevent, we can have our responses, in some cases automate it, and we can have the reconstitution in place to bring the systems back up and running.

Senator CARPER. Give us an example, if you will, of what you called a serious attack scenario.

Mr. PURDY. Well, we would consider an effort that appears to be attempting to access the control mechanism of a control system, say in a waste treatment plant. We would consider that a serious attack because of the ability to change either the manipulation of the activity that it is manipulating and/or the monitoring that could be used to hide if there was a change or a problem. It might affect the sensors' ability to check that out.

More serious situations that you see referenced in last Friday's alert about e-mail trojans that we put out is the exfiltration of data. We are very concerned about—which is basically stealing data from government and the private sector. We believe that is a very significant issue that we are addressing.

You asked a question in terms of some of the activities with the private sector. We are working closely, as I said, with the Process Control Systems Forum. We have had discussions with Siemens, one of the companies that will be testifying later, on some activities in the control systems area and trying to use some of the test beds where we can test the real world activities and capabilities that folks are using and test them in terms of their vulnerability to cyber attack and what kind of measures can be used to help protect them.

So that kind of real world activity—and frankly, some of the activities are not very visible. One of the key things about being a focal point for cyber security is we get classified information, we get law enforcement sensitive information, we get information from the CERT community and from others, and what we try to do is provide real protective measures.

So, for example, there was an attack not too long ago against a private provider that affected a Federal Government customer, and so what we did, when we understood the——

Senator CARPER. Say that again. There was an attack from——

Mr. PURDY. There was an attack against a private sector provider and there was a government account on that system, so we took that information and identified, working with the company, working with law enforcement, identified what we thought was the zone of danger in that situation in terms of the other Federal entities that had access to the same servers in separate accounts. So we had a conference call with about 15 Federal agencies that had not been attacked yet, but to make sure they knew and had specific information they needed so that they could act on it.

Then we issued what is called a Federal Information Notice. That goes to 1,400 Federal agencies. A little less sensitive information, but still, evidence that nonetheless could be used by folks to protect themselves. And finally, a general alert that goes more broadly so that folks could know what to do to secure their systems.

But we don't publicize those kinds of activities. Now, when there is, for example, an attack against a major State that we had to fly a team in to help, we don't publicize that information. We work with law enforcement, the intelligence community to try to bring value, and I share the point from my colleague from GAO that we want to provide value, and as part of this information effort, trying to figure out how to get the value to the private sector and our government partners and our State partners in a way that really is important is something that is very important to us and it builds that trust that you need for people to share, that if you don't go to the press and if you don't publicize these things and you provide real value, that kind of synergy is going to help us all.

Senator CARPER. Thanks very much.

Senator COBURN. Just a couple other questions. Part of your statement was a major priority funding on control systems. Can you elaborate on that for me?

Mr. PURDY. Yes. Our budget for fiscal year 2005 is in the high \$70s of millions. The control systems funding is \$11 million in 2005. The President's budget, which calls for approximately \$88 million for us in 2006, includes between \$15 and \$16 million for control systems. So it is a major effort for us.

Senator COBURN. One other question. Did your Department send a representative to the DOE road mapping exercise?

Mr. PURDY. I don't know offhand.

Senator COBURN. You have got some staff shaking their heads yes. Did DOE send a representative to DHS's framework meeting in Salt Lake City today? I get "yes," too. All right. Thank you.

One of the things that—

Senator CARPER. Mr. Chairman, how do we know that just wasn't members of the audience shaking their heads? [Laughter.]

Mr. PURDY. Yes. I am told that the answer to those questions was yes. I do know that NASCIO, for example, has participated in some of our meetings, building for our national cyber exercise, Cyber Storm, in November, and that kind of outreach is obviously fundamental to the success of these efforts.

Senator COBURN. One other question for you and then a couple more for Mr. Powner. GAO has pointed out that DHS's efforts to promote a trusted two-way communication information sharing have been found lacking by the private sector and some other Federal agencies. In fact, your testimony reflects that the National Cyber Security Division's second priority is cyber risk management, or assessing the threat and reducing the risk. However, you state, with regard to assessing the risk, NCSD collaborates with law enforcement intelligence communities in a number of ways.

My concern is, is your role law enforcement or is it cyber security and prevention, and with a prevention plan? Which is it? Which hat do you all wear?

Mr. PURDY. We are about the business of critical infrastructure protection, and what we have found in our discussions with the major executive agencies, law enforcement agencies, is when there is law enforcement information about an attack, for example, against the control systems, my discussions, for example, with the Assistant Director of the FBI for Cyber was, if you get information in the field about something which is obviously a crime, when there is a successful penetration of a control system or even a targeted attack against a control system, we would appreciate it very much if we would get that information so that we can work the critical infrastructure protection so we can understand what is involved, what is the vulnerability being exploited, so we can share the information, not referring to it in its law enforcement sensitive way, but we can give guidance out.

In addition, we have had situations where law enforcement finds out that there is an attack. We get information about, for example, the source IP addresses of the apparent source of the attack. We work with the intelligence community to have them work the international piece to see if they can trace it back to see what is involved. So it really is critical infrastructure protection, but we have

to share that information with law enforcement intelligence and the CERTs to make sure we can all do our jobs better.

Senator COBURN. But do you then share that with the private sector so that they can enable themselves?

Mr. PURDY. And that is what I am saying that we do in terms of the information bulletins and the alerts that we send out. And as we build our portal into the Homeland Security Information Network, we are going to be able to improve our real-time information sharing, and the best example of that is bringing those nine ISACs in that our information will go into that mix and theirs, as well, and we will share that much more quickly.

Senator COBURN. Mr. Powner, just share with us your view of how serious the threat is to us in terms of our cyber security.

Mr. POWNER. Well, years ago, if you looked at the situation here, we were more focused on hackers who were attempting to break into systems for the sheer challenge or for bragging rights. I agree with Mr. Purdy's analysis. We have organized crime groups that are focused on monetary gains from using cyber tools. We have foreign intelligence services that are using cyber tools for espionage activities. I think the real question out there is where are the terrorist cells in terms of their cyber capabilities. If these folks have the capabilities that we are aware of right now, where are the terrorists?

I think Senator Akaka put it nicely when he mentioned some of the FBI's concerns, which date back many years, looking at what is referred to as swarming attacks, combined attacks where it is not just a cyber attack, but if you have a physical attack where you disrupt the response capabilities via some of the cyber tools, you could then have a very serious situation at hand. So it is real and that threat is growing.

Senator COBURN. Your report was fairly critical of the efforts that are ongoing, and DHS in the response letter to you all states that it has a strategic plan with milestones and performance measures. Where are they insufficient and why are they insufficient?

Mr. POWNER. There is a strategic plan. There is the National Infrastructure Protection Plan. Some of those plans lack milestones. Some of those plans lack key activities. We made recommendations in areas where we saw some weaknesses in their plans. You look at the National Cyber Threat Assessment, vulnerability assessments by sector, and also response plans, not only response plans for the individual sectors, but also when you start looking at combined plans where we have multiple sectors that play in a certain arena.

Probably the best example is if you look at the Internet. If we had a major disruption in the Internet today, the question is, who is in charge of leading that effort to reconstitute the Internet?

Senator COBURN. Who is?

Mr. PURDY. Multiple players, I think, is the answer today. NCSD would play a role. The National Communication System—

Senator COBURN. Let me ask Mr. Purdy that. Who is responsible for putting it back together?

Mr. PURDY. Well, the Secretary of DHS is the incident manager for all incidents in the country. The National Cyber Response Coordination Group that we co-chair helps provide input to the Sec-

retary and provides input to the Interagency Incident Management Group. With NCS, National Communication System, as part of that effort, we would coordinate the efforts across the Federal Government for reconstitution in partnership with the private sector.

Senator COBURN. Two last questions for Mr. Powner. DHS is going to move from \$11 to \$18 million, I believe that was Mr. Purdy's testimony, in 2006, on cyber security.

Mr. PURDY. Eleven to between \$15 and \$16 million.

Senator COBURN. Eleven to \$15 and \$16 million out of \$70 to \$88 million. Is there a problem with priority or is there a problem with funding, in your assessment, as you look at what is going on?

Mr. POWNER. Clearly, there is an issue with priority and there is also an issue with delivery on the budget that is currently allocated. As we pointed out in several areas in our report, there is a situation here where we need to take additional steps—there have been steps in each of the areas that we looked at but there needs to be further steps.

One good example is the National Threat Assessment. In working with the other intelligence organizations, if you look at the FBI Cyber Crime Division and other organizations across the Federal Government, there is a lot of information out there that exists today on the situation associated with the national threat. If we put out, as one example, a National Threat Assessment that the Department agreed to update annually and to provide information on an as-needed basis throughout the area, I think that would go a long ways into building credibility and adding value, where the private sector would clearly view them as a partner in this.

So I think when you look at the current budget, and I think folks up on the Hill—we have had many discussions with them—would like to see more value coming out of the budgets that are currently allocated today.

Senator COBURN. So this threat assessment would be one way to engage the private sector. What are other ways that DHS could engage the private sector?

Mr. POWNER. One other way, I think if you go back to the Internet reconstitution, I think Mr. Purdy talked about or mentioned that NCSD would take a leadership role. There are many folks in the private sector, when you are looking at Internet service providers and telecommunication companies, energy companies, they also would play a major role in that, and if the NCSD, as one example, put together some initial plans, I think the working group that Mr. Purdy mentioned is a step in the right direction, but there needs to be further progress in putting in place response plans that are comprehensive, where the private sector views the Federal Government as a partner.

Senator COBURN. Is there a backup hardware infrastructure in place now if, in fact, the Internet—they would successfully challenge and shut it down, without reprogramming it and everything else, is there a backup infrastructure with which that could be re-assembled quickly on a short-term basis? Do either one of you want to answer that?

Mr. PURDY. Well, I think ESF-II, the communications plan for recovery, is a very robust effort and the telecommunications backbone is the foundation for the Internet. We have done a lot of mod-

eling work in terms of potential disruptions of the Internet and what it would take to carry it out for a long period of time. So I think we are in pretty good shape on that.

I do echo the point that in terms of the priorities, we want to partner more effectively with the private sector on the recovery piece, on the response piece and the information sharing and threat piece. We recognize and we support those conclusions and we are working hard to do that.

Senator COBURN. Have you sent a letter to them saying, how can we do that? Has DHS gone to the private sector and said, how can we partner with you better?

Mr. PURDY. We had two large meetings with the private sector over the last 2 weeks. We had a meeting with the representatives of the Sector Coordinating Council yesterday. We will be meeting within DHS after July 26 to lay out how we are going to move forward to engage. We have had meetings with our lawyers to figure out how we can comply with the Federal Advisory Committee Act, to have private sector folks actually tasked on a working group or a task force.

So we expect to have some concrete progress in setting up those groups, and for each of those groups, identifying milestones and metrics, because the metrics piece is the other big piece that we are moving forward on with our internal and external metrics, and we want the private sector involved with us. So it is not just performance, it is cyber security preparedness, metrics that folks can follow over time to see where we stand, and that is going to help impact the whole National Infrastructure Protection Plan cyber piece.

Senator COBURN. Senator Carper.

Senator CARPER. Just a couple more, if I could. I think I will direct these to Mr. Powner, if I may. I am going to read you something that was prepared in my briefing papers here.

Cyber attacks are launched for monetary gain, for intelligence information, or for the thrill of a challenge. The most commonly used cyber attacks are viruses and worms that are transmitted through the networks and systems to disrupt computer files and programs.

Go back to the first part. Cyber attacks are launched for monetary gain, for intelligence information, or for the thrill of a challenge. In the work that you have done, the study that you have—the time you have invested in this, which of those three, monetary gain, intelligence information, or the thrill of a challenge, seem to predominate?

Mr. POWNER. We don't have specific numbers on that, Ranking Member Carper, but I would say that the monetary gain, when you look at some of the surveys that are done by some of the institutions out there that track this on an annual basis, for monetary gain, those numbers continue to grow year to year. The hacking community, I think they are always going to attempt to hack for the thrill of hacking. The underground community is strong and vibrant. But clearly, when you look for monetary gain, also if you look at recently with online fraud and identity theft, that is also a growing area where there is great concern with security vulnerabilities.

Senator CARPER. I don't know if it was a football coach from someplace in Oklahoma, Oklahoma State University, OSU, or the other OSU, Ohio State University, but one said that—

Senator COBURN. I happen to be an alum of both.

Senator CARPER. I know. I am an alumni of Ohio State. Somehow, I got on the list from Oregon State University. They send me solicitations for money, so I hear from a lot of OSUs.

But one of them once said that the best defense is a good offense. It sounds to me like we play a lot of defense, trying to fend off these cyber attacks. Talk to us about the offense that we are playing, as well. I will start with you, Mr. Powner, and then I will go back over to Mr. Purdy.

Mr. POWNER. Ranking Member Carper, I think if you look at our offensive capabilities, it is probably best if we talked about that in a closed setting.

Senator CARPER. All right. Should we ask our guests to leave? I am just kidding. We won't do it here.

Mr. Purdy>

Mr. PURDY. Let me say the piece of it that I can respond to, because the point is well taken, we are attempting, and I say in my written testimony, to leverage the capabilities of the Federal Government from a cyber defense perspective. That is situation awareness. That is the ability to attribute the source of attacks, the ability to coordinate and prepare for responding to specific attacks and the reconstitution piece. So we are mapping those capabilities across the Federal Government and we are going to identify of those capabilities what do we need to tie into US-CERT?

And third, when there is a cyber incident of national significance, we want to in advance identify the surge capacities and resources that we need brought to bear so we have the full resources of the Federal Government coordinated in partnership with the ISPs and the telecommunications providers, as well. And if you have a good defense, you don't have to respond to other alternatives. We would prefer to try to make ourselves as safe as possible, dealing with the threat as was discussed, but we need to reduce the vulnerabilities because too often, we are not going to know the specific threat information as to who is going to attack us. So we need to prioritize the vulnerabilities under the risk management framework of the Secretary to help mitigate the risks that we face.

Senator CARPER. Sometimes when folks commit crime for monetary gain, they do so because they feel that—there is a risk-benefit situation here. People are willing to take a risk and in return they feel they get a certain potential payoff or a benefit from it.

When it comes to folks that are doing this for monetary gain, I don't know how likely it is that they feel they are going to get caught, prosecuted, go to jail, be fined. Talk to us a little bit about the likelihood that the folks who are doing this for monetary gain are going to be punished and whether or not the punishment is commensurate with the crime.

Mr. PURDY. Who are you directing the question to?

Senator CARPER. Either one of you. Let me start with Mr. Powner.

Mr. POWNER. Would you repeat that, please?

Senator CARPER. I sure will. What I am trying to find out is, somebody is out there. They are going to commit one of these crimes, one of these cyber attacks for money, for monetary gain, and they are thinking through, does this really make sense? Am I going to get something that is worth taking the risk to commit this crime? How likely is it that we are going to catch them, and if we do, is it fair to say that the punishment, the level of punishment, is enough to make them think twice about committing the crime?

Mr. POWNER. A couple comments. One is GAO does not have specific numbers on that, but a lot of these activities go undetected to begin with. So if you start there and say that there are a large number of these attacks that we do not detect, then I think the chances are high that, in fact, they will not get caught because they may not even be detected. Consistent with Andy's comments, I think that is why we are trying to reduce our vulnerabilities, increase our intrusion detection capabilities so that, in fact, we can detect more on a going forward basis.

Senator CARPER. Same question. Mr. Purdy, what I am trying to get at is sometimes when criminals are contemplating a crime, they actually think about, well, what if I get caught? If I get caught, what is likelihood that I will be convicted. If I am convicted, do I go to jail or pay a fine? Is it worth it? And what I am trying to get at is how likely is it that we are going to catch these guys and is the punishment commensurate with the crime.

Mr. PURDY. Well, most of those questions, I would prefer to defer to the Department of Justice. They really have the responsibility in that area.

The point that Mr. Powner referenced, though, in terms of the seriousness with which we view the criminal activity that is occurring in cyberspace and the difficulty of attributing the source of some of the largest attacks we have ever seen, that is all the more reason why we want to focus on reducing the vulnerabilities and working with law enforcement and in the R&D space to try to do a better job of figuring out who is doing these things to us, because obviously in the dynamic of if you don't think you are going to get caught, it doesn't matter what the punishment is.

Senator CARPER. The last question I want to ask is to go back to Mr. Powner. I think it was the May 2005 report called "Department of Homeland Security Faces Challenges in Fulfilling Cyber Security Responsibilities." GAO identified, I think you called it a road map of 13 key responsibilities that were established, both in law and in policy. And my question of you would be, what priorities—and I think the Chairman actually mentioned this before—what priorities, and if you are GAO, should the Department focus on first?

Mr. POWNER. First of all, that was our recommendation, that you take these 13 areas and that they prioritize. But one thing that you could—that could help with the prioritization, I think Mr. Purdy has clearly mentioned a number of their priorities, priority areas on a going-forward basis with building trust relationships and tackling the threat and vulnerability reduction. There are certain areas that the government, and in particular NCSD, controls more than others.

So if you compared threat assessment to vulnerability assessment, vulnerability assessment, they can facilitate the vulnerability assessments, but that really has to be done by the infrastructure owners of the private sector, for the most part. Threat assessment, they control most of that. So in terms of the priorities, there are perhaps some quicker hits with areas that the government controls more than the private sector. So that could be a factor in their prioritization efforts.

Senator CARPER. All right. Gentlemen, thank you.

Senator COBURN. Thank you very much. Thank you for your testimony.

We will now have panel two. Our first witness will be Paul Skare. He is the Product Manager of SCADA, Substation Automation Products for Siemens Power Transmission and Distribution, Energy and Management Automation Division.

With us, also, I will let Senator Carper introduce Thomas Jarrett.

Senator CARPER. Thank you, Mr. Chairman.

I am going to ask Mr. Jarrett when he speaks to just take a moment and introduce the members of his team that are with us here today.

I would just say, because I already talked a good bit about Tom earlier in my opening comments and I appreciate the opportunity to introduce him here today. I was fortunate to serve as Governor for 8 years and one of our real challenges in State Government was to put together at the cabinet level an agency that could help us take our information systems really into the 21st Century, and we struggled with that. We actually had an overall sort of top-to-bottom review of State Government in, I want to say, 1993. We looked at our Information Services Agency, OIS, and tried to determine how we should change it, how we could make it better and to enable us to better serve the folks in our State. I am never convinced we got it quite right.

I think one of the very good things that has been done under the administration of my successor is, I think they have pretty much gotten it right. Part of getting it right is really having the right person to lead that effort, and in Tom Jarrett, I think we have that person.

He brings us to today the perspective of one who has worked in the private sector in these areas, one who has provided great leadership, not just for our State, but I think for others who do his work, his job, his counterparts in other States across the country, and I am really proud of him and the agency and the men and women that he leads.

I thank you for the chance to say those nice words about him.

Senator COBURN. I am struck by the fact that we lost 75 percent of the people that are here, and I am just wondering if all those worked for GAO and DHS, and if they did, no wonder we are not getting where we need to be.

Senator CARPER. They are doing the security for the two witnesses.

Senator COBURN. Thank you both for coming. Mr. Skare, if you would.

TESTIMONY OF PAUL M. SKARE,¹ PRODUCT MANAGER, SIEMENS POWER TRANSMISSION AND DISTRIBUTION, INC., ENERGY MANAGEMENT AND AUTOMATION

Mr. SKARE. Good afternoon, Chairman Coburn, Senator Carper. I am Paul Skare, the Product Manager at Siemens Power Transmission and Distribution. My role is, as we said, managing many of the products that we are talking about here. I am also involved in many standards groups relating to SCADA, or Supervisory Control and Data Acquisitions Systems.

Siemens is a very large company in this product space and we operate in over 190 countries worldwide. In the United States, we have over 70,000 employees and we have operations in all 50 States.

In energy management and automation, we provide software and technologies for the energy market, and these SCADA systems are systems that collect data from all the remote places, the substations, the power plants and other expensive pieces of power equipment, bring them to a central location, and do analysis on this data and turn this data into information so that the operators can then make the right, appropriate actions to correct problems in the field. Obviously, this is a key point for power reliability. Adding more smart applications to these SCADA systems allows you to then do even more detailed analysis and really look at preventing—proactive approaches to preventing blackouts and things.

My testimony today is focusing on identifying some of the potential security vulnerabilities of a SCADA system, some of the activities related to this, and some recommendations to better protect these systems.

While our customers primarily use these systems in the electric sector, many also use the same basic technology for gas, water, and transportation. With some background on this information, I have prepared some appendices that can be submitted into the public record to help the—

Senator COBURN. Without objection, they will be. Thank you.

Mr. SKARE. And I would like to say that in the last few years, I have seen industry and government working better together. What is really noticeable is that a lot of this type of discussion has moved away from the art, or the world called art into a more firm science approach to the issues. and it helps spread awareness and get everyone to speak the same language.

But nonetheless, some of the SCADA vulnerabilities that are issues to look at are obviously remote access. Anytime you have remote access to make it easier to access these devices remotely, it is going to present a vulnerability or the potential for a vulnerability.

Network configurations, the way that you would remotely access these things, of course is very important, to make sure that they are secured, and any minor misconfiguration can create a vulnerability.

Disgruntled employees, whether they are current employees or ex-employees, are a big factor, whether they are mad and they go

¹The prepared statement of Mr. Skare with attachments appears in the Appendix on page 69.

immediately and do something they still have access to, or whether they have just been terminated but they still have access privileges to the system will allow them to go out and do a malicious act.

The discussion earlier about security holes and patches and viruses, worms and so on, is going to be always an issue for this industry because of our high reliance on commercial off-the-shelf technology. Our systems are based on all the standard computers that are available on the market.

Communications should be encrypted. This means if you are using a wide-area network approach, you should have a public-private key infrastructure with encryption and authentication to make sure the data is private and can't be hacked into. You should also make sure that for a lot of these remote devices you are talking to, that you have valid encryption and authentication in place for those, as well.

One of the things that we have talked about in the previous testimonies today is incident reporting, really. How do you know how bad it is when it is unclear how you measure? What are the real incidents? Are you getting a false positive on an attack report? Are the companies that use these systems, are they reporting actual incidents to anybody? Certainly as a SCADA vendor, most of our customers do not want this information public. They don't want to tell us, and they would prefer not to tell anyone because of the potential harm the publicity could bring.

So some of the challenges for these SCADA systems is making sure that all user activity is audited by the individual doing the activity, making sure that there is upgrade kits for older systems to make them secure without having to replace the whole system, making sure all the third-party products involved in these systems are also set up for security and the latest patch is built into those. Again, making sure that we have the secure communications, both over WANs and over slower dial-up-type access.

And finally, making sure that a lot of the low, weak devices that you are talking to have the ability to have encryption between them so that when you are talking from a control center out to an RTU or a remote device that is bringing the data in, even if it is a really old one, that you can still get a secure communications and not have concerns from that regard.

Some of the recommendations that will help achieve securing these systems is making sure that business processes are aligned with security in mind. Now, NERC has done a lot to create some security policy where it is sent to foster requirements for security policies, but not necessarily—with the energy bill now, the enforcement becomes a possibility for NERC to be able to address these issues. Today, the enforcement is only a voluntary enforcement, and so for a utility to have a security manager and a security awareness program and making sure there are no little yellow sticky notes with user names and passwords laying around is an important aspect of security.

Types of SCADA systems also have some challenges on the different types of security because an electric SCADA system will be processing information every one or two seconds, pulling that information in and doing analysis on it, while something on a gas pipeline system might only need to pull that data in once every 10 min-

utes. So a gas pipeline system can have a higher level of encryption and still get its data in time, but for an electric power system, when you are talking about collecting data at perhaps once every second, you can't block the access of the data by having so much encryption that it slows down the availability of the data.

So with that regard, one of the recommendations is to foster some research into that area so that for these low-powered devices, that includes some of the wireless devices that are out there now, too, because more and more, you are seeing sensors connected into the system through a wireless connection before they come upstream to the control center, and right now, there is a need for research in the security of these wireless communications.

Another recommendation is to have a secure way of reporting both the threats and the incidents in these systems. So, for example, whether someone has a threat available, it is not necessarily accurate that everyone is aware of that threat, and also, if a utility is faced with an attack or a security incident, there is no mandate that says they have to report that to anyone. And if there was a way for these incidents to be shared along with the vendors that make these systems, it would allow us to more rapidly respond to fixes for these incidents.

Another issue is incentives for the utilities when they secure their systems. If there was an approach that would ensure that the culture at these utilities had the mindset of securing their systems in a way to help their cost recovery on those through either tax incentives or some such mechanism, would be helpful, I think, for the electric utilities.

Federal and State cooperation, it is not just the people we have talked about today, but each State Public Utility Commission is also involved in the operation of these electric utilities and the co-operation and perhaps public outreach in these areas with the Public Utility Commissions would be of benefit.

And then there is also non-jurisdictional utilities also could be useful to be brought into the fold with the security discussion.

Another recommendation is Department of Homeland Security and Department of Energy have some similar programs and it would be useful, I think, to have them perhaps a little more coordinated or merged together.

We heard earlier today about the Control System Security and Test Center, and there is also the National SCADA Testbed, both out at Idaho National Laboratory. And while Siemens has a system out there, I think that it would be useful to have these programs combined and have a longer-term funding approach for them so that you can see that as these vendor systems get out there and the vendors produce fixes and patches for them, that over time, you can verify that these systems are really getting secured. But this is not a one-year type of approach. This is a multi-year activity.

The other thing that would be useful is if the different national laboratories were a little bit more in sync and didn't appear to be competing. For example, Idaho National Lab, Sandia National Lab, specific Northwest National Lab and Oakridge, which all have some relevance to this subject, in fact, three of them do have a partnership for the National SCADA Testbed, but in overall, there

has still in the past been some confusion as to who is taking what role in this activity.

The various management changes and reorganizations have had an impact, also, on making sure you know who you are talking to in order to accomplish various tasks in this arena.

Senator COBURN. Let me get you to summarize, if you would.

Mr. SKARE. OK. Absolutely. The final point is that a risk-based approach is, I think, the most effective approach to these issues.

Finally, I would like to say that Siemens is very supportive of these activities and will continue to be made available and to assist and to work in the area to secure the Nation's critical infrastructure. Thank you.

Senator COBURN. Secretary Jarrett.

**TESTIMONY OF THOMAS M. JARRETT,¹ SECRETARY AND
CHIEF INFORMATION OFFICER, DEPARTMENT OF TECH-
NOLOGY AND INFORMATION, STATE OF DELAWARE**

Mr. JARRETT. Thank you. At Senator Carper's request, first, I will introduce the folks that came along with me. First is Elayne Starkey, the Chief Technology Officer for the Department; Michele Ackles, who is my Deputy in the Department; and I would also like to introduce Shay Stautz, who is here with me from NASCIO, so I am glad that they joined me today.

Thank you for inviting me to appear before you today. I appear in two capacities, first representing the great State of Delaware as Secretary of Delaware's Technology and Information Agency, and second, as the current President of the National Association of State Chief Information Officers, or NASCIO.

First, I would like to thank Chairman Coburn and a special thanks to Delaware's Senator Tom Carper for inviting me to speak with you today. As Delaware's CIO in charge of all State Government information and communications technology, my highest priority is cyber security.

The security of Delaware's information technology system is critical to the well-being of our State as a whole, not just the business of the State, but also its economy. Further, from a Federal perspective, Delaware's information system is key to providing Federal services to our citizens and supports homeland security efforts.

In the most simple of terms, keeping those who would wish to do us harm out of our network and systems is the primary challenge of IP security staff in Delaware and across the Nation. Delaware's State network may be small in comparison to some other States, yet we are responsible for over 130,000 users, representing all three branches of government, including our law enforcement, first responder, and educational communities.

We have recently deployed new software that permits us to check network events on a daily basis and we fend off nearly 3,000 daily attempts at entering our network. I would like to repeat that, nearly 3,000 attempts a day to invade our network. As you will see in the documentation that I have attached to my statement, these numbers are not out of line with what other States are seeing.

¹The prepared statement of Mr. Jarrett with attachments appears in the Appendix on page 105.

Because of our extreme diligence, we have not had a significant intrusion into our network. Keeping those that would wish to do us harm out of our network requires multiple layers of protection. While it is rarely a terrorist in the traditional sense of the word that threatens the State network, we do not focus specifically on who is trying to infiltrate our network. Rather, our goal is to keep all those with bad intentions from entering our system.

Without lapsing into too many technical terms, we deploy a number of different hardware and software products to protect our networks. We scan, scan, and scan again all traffic coming into the network. We search for viruses, spam, spyware, and other recognized problems.

Delaware is proactive in establishing collaborative partnerships at the Federal and local level. We have a working relationship with the FBI, who performs vulnerability audits and scans for us. We collaborate with the private sector, as well. Delaware was the first State to become part of an extensive security cooperation program that Microsoft has established.

During times of heightened security alerts, like that resulting from the recent terror incidents in London, we also raise the bar on cyber security. We increase our vigilance and our monitoring because we are well aware that a virus that begins in Asia can propagate to the United States in a matter of a few short hours. In a very short period of time, it is possible for a system that has been not hardened or properly maintained to be completely overrun.

Now, what does the future hold? Unfortunately, I have to state that I believe that threats to cyber security will only increase and we will face continuing attacks and attempts on multiple fronts. State IT officials must continually adjust how and what is filtered, blocked, and monitored. New threats appear almost daily and they can, in a matter of seconds, render services we have all come to depend upon, like e-mail and web browsing, completely unusable. In the worst case scenario, without proper protection, an attack could potentially cripple or completely shut down an entire State Government.

While we must understand that all critical infrastructure is the same by its very nature, critical, whether it is a roadway system or an information network, infrastructure is about moving people and information and a State's network infrastructure is equally as important as its highways, electric power grid, or mass transit system.

I will conclude my remarks with a few words about what NASCIO is doing. NASCIO is working with the States to get a comprehensive picture of the challenge that cyber security represents. We have produced a series of snapshots into what a few States are doing. Let me share just a few experiences from my CIO colleagues.

Michigan reports that nearly 32 percent of its incoming e-mail carries viruses, while Montana reports a rise from 93 attempted virus infections in 1997 to nearly 45 million in 2005. Kansas blocked 600,000 intrusion attempts over a 3- to 4-hour time period during one recent attack.

Protecting critical IT infrastructure does not come cheaply. We estimate that my Department spends \$5 million annually, or 15

percent of my annual budget, on cyber security. A recent Statewide assessment in North Carolina revealed that approximately \$50 million was needed to implement a statewide security plan.

NASCIO believes that the Federal Government and the States must increase collaboration in facing these threats which we share in common. NASCIO applauds last Wednesday's announcement by Secretary Chertoff that he will create an Assistant Secretary for Cyber Security within the reorganized Department. NASCIO supported the calls for such a position and has endorsed past legislative efforts seeking to create the position. In fact, State CIOs have made addressing deficiencies in public sector cyber security their No. 1 item on our Federal agenda. We believe that the creation of a higher-profile position for cyber security within DHS is an important statement to the Nation as a whole.

Having provided you with this background, NASCIO comes prepared to offer the Subcommittee one substantive step that it can take forward toward improving intergovernmental cyber security. NASCIO has provided Subcommittee staff with language that encourages the Secretary to have DHS revise the existing strategy and assessment process to include requiring a cyber security preparedness plan from each State and each State's CIO. We feel that closing the cyber security planning gap in the near term, and especially before the next round of grant making gets underway, is the single most important issue facing our sector today.

Finally, NASCIO points out that information systems in general are the only part of the Nation's critical infrastructure that is under attack everywhere, all the time, and these attacks are inflicting millions of dollars in damage. Cyber attacks, even those without terroristic intent, could disrupt government's operations in general or homeland security mission critical systems specifically. It is our duty to secure these systems from all types of threats, regardless of the intent behind them, and as soon as possible.

As the CIO for the State of Delaware and the President of NASCIO, I appreciate the work that the Subcommittee is doing in confronting this national challenge. Thank you.

Senator COBURN. Thank you, Mr. Jarrett.

Senator Carper has to leave and I am going to defer to him for the first set of questions.

Senator CARPER. Thank you very much, sir.

Again, to our witnesses, thanks a lot for coming and for really excellent testimony in ways that even I could almost understand. Sometimes when we have people testify on these subjects, I am not sure I understand the words. As Mrs. Einstein used to say, Albert Einstein's wife, "Mrs. Einstein, do you understand what your husband is saying or talking about?" And she said, "I understand the words, but not the sentences." I think for your testimony, for the most part, I understood not only the words but, in many cases, the sentences.

I want to return to a question I asked the last panel and never got the answer I was looking for. I raised the issue of a football coach who is looking for ways to provide a good offense, and not just a good defense. We had a big middleweight championship fight out in, I think it was Las Vegas, this past weekend. A guy who de-

fended his title, I think 20 times, was unsuccessful in title defense No. 21.

Senator COBURN. Fighting is not good for you.

Senator CARPER. That is what I have heard, at least fighting against those guys wouldn't be good for us. But as I listened to this testimony, I am reminded of a boxing match, maybe even a football game, where one side is on defense the whole time and you never get the ball to go on offense. I am reminded of a fight where you have got one guy is permitted to throw all the punches and the other guy just basically has to take them. Am I misreading this? Are there ways that we can fight back effectively? It seems that all we do is play defense, and I think we are pretty good at it, it sounds like we are very good at it, but I like to play offense, too. Are we? Should we be?

Mr. JARRETT. Well, I would say from a State perspective, I think we are beginning that process. We have spent considerable dollars over the last several years building a very strong defense. But the real issue here is more in trying to identify the people that are actually trying to get into our networks, they hide themselves very effectively. So you need to have the resources and the money to then go after them, and I happen to be a believer that we should be going after them, but they are very difficult to find. In our case, as quickly as we make changes to our system, we see changes that have already countered those changes. So very definitely, I would hope that we will begin to take a much more offensive approach, but it is very difficult.

Mr. SKARE. I think that we have a very large installed knowledge now with intrusion detection systems, but now the latest thing that is coming along is intrusion prevention systems. So what it is, it is trying to take a look at the known signatures of some of these attacks and try and prevent them as they are happening, or the so-called zero day defense that is really happening. And when you combine that with a defense in depth approach to your control system, you have a much better chance of really trying to proactively stop them as it happens, although I would say that there is still a long ways to go there.

But, for example, when you look at some of these control systems, they use quite common standardized protocols so that all the different systems can talk to each other and these are mostly publicly available, so we are taking a look at how do you scan real time these data communications and prevent things from happening real time.

Senator CARPER. All right. A question, if I could, this would be for Secretary Jarrett. I believe in your testimony, I think I heard you say that some 15 percent of your Department's budget is just for cyber security initiatives. Last week, Secretary Chertoff said, I believe in this hearing room, not only the establishment of the Assistant Secretary for Cyber Security and Telecommunications, but he talked about dedicating some Federal resources to help the efforts across the board. Let me just ask, what additional resources do you believe that the Federal Government, if any, should allocate, if any, for cyber security initiatives?

Mr. JARRETT. Well, I think there are two pieces of that. I have read some of the numbers as far as dollars that they are talking

about appropriating to that. When I compare them in direct comparison to what I spend, my comment would be that I don't think it is enough. So I would hope that the appropriations that they are going to put towards cyber security would be much larger than what I, at least from what I have currently seen.

Senator CARPER. It would also be great if, whether the allocations are huge or large or moderate, it would be great if they were doing something that sort of complemented what you were doing with this data, not necessarily duplicate or replicate.

Mr. JARRETT. And that was going to really be my second thought, which is I heard the comments and what was honestly striking to me was the fact that though there was a lot of talk about connections between agencies and all that, there was no mention of connection really to the States. And I would argue that the States are really the first line of defense when it comes to, whether it is first responders and those kinds of things. We are kind of out front on a lot of areas, working in the area of cyber security. So we would like to work much more effectively with them in the future. I think that would be a tremendous approach if we could finally, or at least ultimately, reach that point.

Senator CARPER. One other thought, Mr. Chairman, comes to mind. I think it was Lincoln who used to say, the role of Government is to do for people what they cannot do for themselves. Maybe a reasonable role for the Federal Government here, for the Department of Homeland Security, is to do for States what you cannot do for yourselves, or for the private sector, for that matter.

One last question, if I could, for Secretary Jarrett. I believe your first task, as I recall, as Secretary was to transform Delaware's Office of Information systems to this Department of Technology and Information. You hand picked and hired an entirely new organization that is built on a market-based compensation plan where individuals are compensated based on their performance within the Department. You also did away with many middle management positions. You enabled employees to be more connected with the end result.

I would just ask what suggestions you might have, really for the Department of Homeland Security, for our Federal agency, for your big brother, if you will—that probably has the wrong connotations—but for Homeland Security in finding and retaining the most highly qualified individuals to protect our Nation's critical infrastructure.

Mr. JARRETT. I have a pretty basic thought about that and it comes down to the most basic thing, which is pay. One of the key approaches that Delaware took was to be able to pay our people within the Department what the market, and what they would literally get in the market if they were to go outside of working in State Government. We found that to be very effective, because in the end, if you are going to be effective in managing, working these kinds of issues, then you have to have very good people, and if they are going to be accountable, then you have to be willing to pay them, or otherwise very likely they either won't come to you in the first place, or if they do, they won't remain very long.

So we have found that our pay structure has been probably one of our greatest assets because it has allowed us to hire very excel-

lent people who are more than willing to stay because we are very competitive.

Senator CARPER. Great. Mr. Chairman, thanks for letting me lead off here. And again to Secretary Jarrett, it is great to see you.

Mr. JARRETT. Thank you.

Senator CARPER. Thank you for you and your team, who are representative of the great work you are doing on behalf of our State and for, I think, the wonderful example you are providing to a few other States. Congratulations. He is not only Secretary, Mr. Secretary, but he is also Mr. President of his national organization. It is not every day we get to do that. Thank you both.

Senator COBURN. The Senator from Delaware, are you proposing waiving government parameters limiting the ability to increase pay and pay for performance in Homeland Security? That is something our President has been trying to do here for some period of time.

Senator CARPER. When we have a private conversation with our earlier panel on the matters they couldn't discuss, let us bring that one up, too.

Senator COBURN. OK. Good answer. [Laughter.]

Senator COBURN. Mr. Skare, here is how my staff assesses you. He is a world class operational control systems technology expert. He works for one of the world's largest manufacturers and leaders in control systems. So I want to ask you very frankly, do you have a good working relationship with DHS? Are they communicating the way they should with you? Are you allowed to get information that is helpful to you when you should, and do you feel comfortable sharing information with them?

Mr. SKARE. Well, that is a very good question. I think that there has been some changes in management. I originally was contacted and had been working with Mike Lombard in the Department of Homeland Security, and then that had shifted over to David Sanders. I think as some of the activities go on—for example, the DHS did invite me to the road map meeting we had last week in Baltimore, and I think that it was a very good meeting for sharing ideas with the DHS people.

My experience with DHS is that they are very focused on moving quickly. But as far as sharing any detailed information, I do not have any specific threats shared with me of any sort.

Senator COBURN. So, in other words, there may be a threat to one of the systems that you are looking at that they know about that you don't know that could maybe enhance your ability to do the job better as a vendor for those items, yet you are not seeing the feedback loop coming on that.

Mr. SKARE. That is right. I have seen no feedback in that area.

Senator COBURN. Is that not something that we want to happen?

Mr. SKARE. I believe it is. I know that I actually had this discussion with one of the DHS people last week and we discussed if it meant that we should get security clearance, or maybe there is a new type of clearance that could be created, a trusted type of information sharing line that could go on. But the discussion was still an ongoing discussion.

Senator COBURN. Well, if 85 percent of our cyber is in private hands, we are going to have to talk to the private sector. That would mean 15 percent is in the State and Federal hands and

other entities. We are going to have to communicate, and I was most concerned about GAO's testimony as this lack of confidence, because if there is not confidence with DHS, then you as a spokesman or lead individual for your company are going to be somewhat hesitant to share with them information. And so if we can't get past the—it is kind of like marriage. If you can't get past the trust deal, you never get anywhere. So if we can't get there, this can build and this can grow if we have a working relationship. I am concerned.

Have you noticed anything, Secretary Jarrett, in terms of your ability to relate and a level playing field and informational exchange that you could offer us?

Mr. JARRETT. We have found that the information exchange has been very difficult. That is why we have built strong relationships with most of our business partners. I can tell you that most of the threat data that we get today, we get from those business partners and through US-CERT, but not directly from the Department.

Senator COBURN. Through the US-CERT?

Mr. JARRETT. Right.

Senator COBURN. OK. And did either of you gentlemen happen to see the article yesterday in the *Wall Street Journal* where they talked about the trojans? I thought it was a very informative article for the public because it is us and our personal computers that are being used to scam everything else in the world and used to, what do they call it, bot—

Mr. JARRETT. Bots and zombies and—

Senator COBURN. Yes. I would also note that DHS is not in here anymore for them to hear your testimony, which is concerning for me, because that is one of the areas, we are sponsoring this, we have 15 people from DHS attend a hearing, but when they are through testifying, then they are not here to hear what the rest of the panel says so we don't get the information. So that says you don't build trust if you can't communicate, and if you aren't going to listen, you are never going to be able to communicate. So I am somewhat critical of that.

Mr. Jarrett, does your office have regular contact with the National Cyber Security Division at DHS?

Mr. JARRETT. We do not. We do on a kind of hit-or-miss basis. We do a lot of things. We are members of the MS ISAC, which is the 50-State group that has come together, but not directly with them.

Senator COBURN. Did I hear you right a moment ago that you thought there should be a requirement for each State to have a preparedness plan?

Mr. JARRETT. A cyber security preparedness plan, absolutely.

Senator COBURN. And should that be contingent on their DHS grant?

Mr. JARRETT. I think it should be tied directly to the grant process. What has been difficult in the current grant process is that little of that money is going towards cyber-related issues. I can tell you, in the 3 years that monies have come out in my State, I just for the first time got a small amount of those dollars for some cyber work that we are doing. It has been driven toward other directions, and though I understand that and respect that, I think that we

need to also understand that the cyber aspect of this is absolutely critical.

All of our systems and everything that—I run all of the systems for all the first responders, the State police, everyone, so during time of greatest need, if my systems go down, they literally have no access to any of the information that they will require.

Senator COBURN. And you already answered this somewhat, but I want to ask you again, and I find it strange. Fifteen to \$16 million of this next year's budget for DHS, and you are going to spend \$5 million, and you say to set a State up, it is going to take \$50 million just in programming the structure and observations and diligence. I am kind of appalled that that is the priority. Are you?

Mr. JARRETT. I am concerned about the priority, absolutely. I mean, we are very happy to see that they have established the Assistant Secretary for Cyber Security. That is something that we have pushed for for a long time. But with it must come the right funding to be able to do the job correctly and the amount of money, at least that I have seen, concerns me.

Senator COBURN. How are you all at the State of Delaware informed of a fast-moving cyber threat? How do you find out, other than your own observation and blocking and monitoring technique?

Mr. JARRETT. Two primary ways today, neither of which are the Department. One is through the MS ISAC structure that was created about 2 years ago—

Senator COBURN. Is that fast? Do you get that on a real time basis?

Mr. JARRETT. We get that on a real time basis. It has become a very dynamic group. We meet once a month, and so we have built a structure within the States that allow us to share information on a very rapid basis.

We also get it from our vendors through our cooperative program with companies like Microsoft and Oracle and others. And all of my key security folks are obviously also connected to the US-CERT process, as well.

Senator COBURN. Is that timely, the US-CERT process, or does it come hours or days after the fact?

Mr. JARRETT. We are actually finding the US-CERT process to be quite timely—

Senator COBURN. Good.

Mr. JARRETT. So we have been very pleased with that at this point. Timeliness, obviously, in our business, is absolutely critical, given the fact that we are talking about threats that—we are not talking about days, we are talking about minutes and hours.

Senator COBURN. And going back to your testimony, Mr. Skare, if you are talking about a power generation facility and they are monitoring sequentially, there is not the technology for encoding or encrypting instantaneously that information so that you can stay on a real time basis without putting that facility at risk?

Mr. SKARE. There are ways to do that for network connections, although a lot of the standards are still lacking in approval from an approval perspective, and many utilities are reluctant to roll out technologies like that until they have been standard and approved.

Senator COBURN. And who holds that approval?

Mr. SKARE. It depends. In this case, there is international approval as well as U.S. approaches. In the international arena, it is the International Electrotechnical Commission. On the U.S. side, the standard that most U.S. utilities are going to be looking toward is one set by NERC.

Senator COBURN. OK. I can't help but think about the television show "24" and how closely you were involved in that. Part of our risk—there has been \$60 billion spent by the U.S. Government on IT in this last year, \$60 billion by the Federal Government. That is a big sum of money. And yet it doesn't seem that we are a whole lot more secure. We may be faster and we may be moving information around, but the more IT we have, the more risk we have if it is vulnerable.

What is the budget for the State of Delaware on IT? Do you have any idea?

Mr. JARRETT. Well, about \$300 million.

Senator COBURN. A year?

Mr. JARRETT. A year.

Senator COBURN. And that is both hardware and software, the whole—

Mr. JARRETT. That is everything.

Senator COBURN. That is the whole thing. All right.

Mr. Skare, you talked about business process. What motivates, or what would motivate a company to make an investment in cyber security to protect their critical infrastructures, those that have not?

Mr. SKARE. I think those that have not, any type of business case where you can show them where the loss or the damage to their business due to such an incident would result in a negative impact on their business. For example, if an attack took down a particular substation and those customers were without power for a certain amount of time, you would have not only the lost revenue due to the power outage, but you would also have then the damage to the reputation. And quantifying those in terms of a business case would go a long way to help.

Senator COBURN. And so you all are seeing more that your business is good, is that correct?

Mr. SKARE. Interestingly enough, common sense might dictate that after a major event, such as the blackout in 2000, it would spur investment in these areas. However, there was a certain amount of reluctance to spend purely so that it wasn't seen as a reaction or as a sign of weakness. So it is kind of a balancing act.

Senator COBURN. I want to thank both of you for your testimony and for staying as long as we have. I appreciate you coming and giving this information.

We may submit some questions to you in writing. We very much appreciate if you would be timely in your response to those.

Thank you very much for attending. The meeting is adjourned.

[Whereupon, at 3:44 p.m., the Subcommittee was adjourned.]

A P P E N D I X

**Written Statement of
Donald (Andy) Purdy, Jr.
Director (Acting), National Cyber Security Division
Information Analysis and Infrastructure Protection Directorate
U.S. Department of Homeland Security**

**Subcommittee on Federal Financial Management, Government Information, and
International Security
Committee on Homeland Security and Governmental Affairs
United States Senate**

July 19, 2005

Good morning Chairman Coburn and distinguished members of the Subcommittee. My name is Andy Purdy, and I am the Acting Director of the National Cyber Security Division (NCSD) within the Department of Homeland Security. I am delighted to appear before you today to share with you the work of the NCSD and those with whom we are partnering to secure our national cyberspace and critical information infrastructure. In my testimony today, I will provide an overview of NCSD, our operating mandates, our mission and goals, our priorities, and the programs in which we are engaged to meet those missions and goals. Much of the information in my testimony today is reflected in the recent Government Accountability Office (GAO) report 05-434, which focused on cyber security responsibilities and in our response.

Introduction: DHS and Cyber Security

As you may know, Secretary Chertoff has proposed a new Assistant Secretary for Cyber Security and Telecommunications as part of his six point agenda for the Department, announced on July 13th. As it currently stands in DHS, the core cyber security activity is located in the Information Analysis and Infrastructure Protection (IAIP) Directorate. The IAIP Directorate includes the Office of the Chief of Staff; the Information Sharing and Collaboration Office (ISCO); the Office of Information Analysis (IA), the primary gathering and analytic center for threat information and intelligence within DHS; the Homeland Security Operations Center (HSOC), the primary national-level hub for domestic operational situational awareness, common operational picture, communications, information fusion, and coordination pertaining to the prevention of terrorists attacks and domestic incident management; and the Office of Infrastructure Protection (IP). The Office of Infrastructure Protection has four component divisions, including the Infrastructure Coordination Division (ICD), the Protective Security Division (PSD), the National Communications System (NCS), and the National Cyber Security Division (NCSD). Within the Directorate, IA, IP, and the HSOC work together to share intelligence and other information as well as to coordinate our efforts to mitigate our vulnerabilities.

In today's highly technical and digital world, we recognize that attacks against us may manifest in many forms, including physical and cyber. In addition, we recognize the potential impact of collateral damage from any one attack to a variety of assets. This interconnected and interdependent nature of our critical infrastructure makes it difficult – not to mention irresponsible – to attempt to address the protection of our physical and cyber assets in isolation.

As such, IAIP takes a holistic view of critical infrastructure vulnerabilities and works to protect America from all threats by ensuring the integration of physical and cyber approaches.

NCSD was created in June 2003 to serve as a national focal point for cyber security and to coordinate implementation of the *National Strategy to Secure Cyberspace* (“the Strategy”) issued by President Bush in February 2003 that set out a national framework for addressing various aspects of cyber security. The Strategy established the following five national priorities for securing cyberspace:

- Priority I: A National Cyberspace Security Response System
- Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program
- Priority III: A National Cyberspace Security Awareness and Training Program
- Priority IV: Securing Government’s Cyberspace
- Priority V: National Security and International Cyberspace Security Cooperation

In December 2003, President Bush further solidified NCSD’s mandate as a national focal point for cyber security by issuing Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD-7), which calls for DHS to “...maintain an organization to serve as a focal point for the security of cyberspace....”¹ HSPD-7 also established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. Furthermore, HSPD-7 laid out how DHS should address critical infrastructure protection, including “...a summary of activities to be undertaken in order to: define and prioritize, reduce the vulnerability of, and coordinate the protection of critical infrastructure and key resources.”²

To meet this mandate, IP embarked on the development of the National Infrastructure Protection Plan (NIPP) that will serve to address critical infrastructure protection in the seventeen (17)³ identified critical infrastructure sectors and key resource sectors. The interim NIPP issued in February 2005 encompasses a risk management framework for public and private sector stakeholders to work together to identify critical assets in each of the sectors, prioritize them, conduct vulnerability assessments in each of the prioritized sectors including identification of interdependencies among them, and provide priority protective measures that owners and operators of those assets should undertake to secure them. The final NIPP is expected to be released later this year.

HSPD-7 outlines “Sector Specific Agencies” (SSAs) for each of the critical infrastructure sectors, with DHS serving as the overall coordinator for the NIPP program. The private sector-

¹ Homeland Security Presidential Directive 7, December 17, 2003; <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>; Para (16).

² Homeland Security Presidential Directive 7, December 17, 2003; <http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html>.

³The NIPP identifies the following Critical Infrastructure Sectors and Key Resources: Food and Agriculture; Public Health and Healthcare; Drinking Water and Wastewater; Energy; Banking and Finance; National Monuments and Icons; Defense Industrial Base; Information Technology; Telecommunications; Chemical; Transportation Systems; Emergency Services; Postal and Shipping; Dams; Government Facilities; Commercial Facilities; Nuclear Reactors, Materials, and Waste.

led Sector Coordinating Councils (SCCs) and/or Information Sharing and Analysis Centers (ISACs) work with each SSA; and the SSA's are the chairs of the respective Government Coordinating Councils (GCC), which represent the government agencies that have a role in protecting the respective sectors. DHS SSA responsibilities include the Information Technology Sector and the Telecommunications Sector. Specifically, NCSD coordinates the Information Technology Sector, and the NCS coordinates the Telecommunications Sector. Reflecting the increasing convergence between these two communications sectors in today's market, NCSD and NCS work together closely to coordinate all efforts to protect the nation's critical cyber systems and the telecom transport layer. In addition to its IT sector responsibility, NCSD is responsible for providing cyber guidance to all sectors to include the information infrastructure vulnerabilities they may have as well.

Given today's interconnected environment and DHS's integrated risk-based approach to critical infrastructure protection, NCSD's mission is to work collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets. To meet that mission, NCSD developed a Strategic Plan that establishes a set of goals with specific objectives for each goal and milestones associated with each objective. The Strategic Plan goals, which are closely aligned with the *National Strategy to Secure Cyberspace*, HSPD-7, the interim NIPP, and the Cyber Annex to the National Response Plan, are as follows:

1. Establish a National Cyberspace Response System to prevent, detect, respond to, and reconstitute rapidly after cyber incidents;
2. Work with public and private sector representatives to reduce vulnerabilities and minimize severity of cyber attacks;
3. Promote a comprehensive awareness plan to empower all Americans to secure their own parts of cyberspace;
4. Foster adequate training and education programs to support the Nation's cyber security needs;
5. Coordinate with the intelligence and law enforcement communities to identify and reduce threats to cyberspace; and
6. Build a world class organization that aggressively advances its cyber security mission and goals in partnership with its public and private stakeholders.

To meet these goals, NCSD is organized into four operating branches: (1) U.S. Computer Emergency Readiness Team (US-CERT) Operations to manage the 24x7 threat watch, warning, and response capability that can identify emerging threats and vulnerabilities and coordinate responses to major cyber incidents; (2) Strategic Initiatives to manage activities to advance cyber security in critical infrastructure protection, control systems security, software development, training and education, exercises, and standards and best practices; (3) Outreach and Awareness to manage outreach, cyber security awareness, and partnership efforts to disseminate information to key constituencies and build collaborative actions with key stakeholders; and (4) Law Enforcement and Intelligence to coordinate and share information between these communities and NCSD's other constituents in the private sector, public sector, academia, and others, and also to coordinate interagency response and mitigation of cyber security incidents. Together, these branches make up NCSD's framework to address the cyber security challenges across our key stakeholder groups and build communications, collaboration, and awareness to further our

collective capabilities to detect, recognize, attribute, respond to, mitigate, and reconstitute after cyber attacks.

Cyber Security Priorities: Response and Risk Management

The *Strategy* and HSPD-7 provide NCSD with a clear operating mission and national coordination responsibility. To carry out the mission and those related responsibilities, NCSD has identified two overarching priorities: to build an effective national cyberspace response system and to implement a cyber risk management program for critical infrastructure protection. Focusing on these two priorities establishes the framework for securing cyberspace today and a foundation for addressing cyber security for the future.

Priority 1 – Cyber Incident Management: A National Cyberspace Response System

A core component of NCSD and our effort to establish a National Cyberspace Response System is the US-CERT Operations Center. US-CERT was established in September 2003 as a partnership between DHS and the public and private sectors to address cyber security issues. Beginning as an initial partnership with the Computer Emergency Response Team Coordination Center (CERT/CC) in Carnegie Mellon University's Software Engineering Institute, US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our nation's cyber infrastructure. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from cyber incidents and attacks across the United States, as well as from the cyber consequences of physical attacks or natural disasters.

US-CERT has four major programs of activity. First, US-CERT is DHS's 24x7x365 cyber watch, warning, and incident response center, and provides coordinated response to cyber incidents, a web portal for secure communications with private and public sector stakeholders, a daily report, a public website (<http://www.us-cert.gov/>), and a National Cyber Alert System, which provides timely, actionable information to the public on both technical and non-technical bases. Second, US-CERT conducts malicious code analysis, provides malware technical support, and conducts cyber threat and vulnerability analysis. Third, US-CERT manages a situational awareness program that includes the Einstein Program for monitoring network activity in the federal agencies, currently operational at three agencies, with five pending deployments within the next four to six months; and, an Internet Health and Status service used by 50 government agency computer security incident response teams. Fourth, US-CERT manages programs for communication and collaboration among public agencies and key network defense service providers. In line with NCSD's close working relationship with NCS, US-CERT works closely with the National Coordinating Center for Telecommunications (NCC) to address and mitigate cyber threats including response and recovery. U.S. CERT also maintains a presence in the HSOC to ensure coordination throughout DHS.

As noted, NCSD has initiated a number of activities specifically to assist federal agencies in protecting their cyber infrastructure. NCSD established the Government Forum of Incident

Response and Security Teams (GFIRST) to facilitate interagency information sharing and cooperation across federal agencies for readiness and response efforts. GFIRST is a group of technical and tactical practitioners of security response teams responsible for securing government information technology systems. The members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. The purpose of the GFIRST peer group is to:

- Provide members with technical information, tools, methods, assistance, and guidance;
- Coordinate proactive liaison activities and analytical support;
- Further the development of quality products and services for the federal government;
- Share specific technical details regarding incidents within a trusted U.S. Government environment on a peer-to-peer basis; and
- Improve incident response operations.

GFIRST meets on a regular basis and held its first annual conference in April 2005 with more than 200 participants from federal, state, and local governments. The conference was a major success for US-CERT, and GFIRST has established further lines of communications across organizations. The technical workshops and speakers stimulated many technical interchanges regarding cyber first responder activities. In another step forward, GFIRST held its first classified threat briefing with DHS IA, the Central Intelligence Agency, Department of Defense, and National Security Agency in June 2005.

US-CERT utilizes a secure collaboration platform, which is being intergrated into the Homeland Security Information Network (HSIN), to support cyber information sharing and collaboration among the GFIRST community, and other communities, such as the ISACS. This secure platform bridges the gap between Government participants as well as participants from the ISAC and other private sector partners.

In addition to GFIRST, NCSD worked with DOD and DOJ to help form the National Cyber Response Coordination Group (NCRCG) to provide a federal government approach to coordinated cyber incident response. We created a Cyber Annex to the recently issued National Response Plan (NRP)⁴ that provides a framework for responding to cyber incidents of national significance. As such, the Cyber Annex formalized the NCRCG as the principal federal interagency mechanism to coordinate preparation for, and response to, cyber incidents of national significance. The co-chairs of the NCRCG are DHS/NCSD, the Department of Justice, and the Department of Defense. An additional 13 federal agencies with a statutory responsibility for and/or specific capability toward cyber security, including the intelligence community, comprise the membership. NCSD serves as the Executive Agent and point of contact for the NCRCG. The NCRCG has developed a concept of operations (CONOPS) for national cyber incident response that will be examined in the National Cyber Exercise, *Cyber Storm*, to be conducted by NCSD in November 2005 with public and private sector stakeholders.

In addition to its CONOPS and incident response mechanism, the NCRCG is reviewing capabilities of federal agencies from a cyber defense perspective to better leverage and

⁴ <http://www.dhs.gov/dhspublic/display?theme=15&content=4269>

coordinate the preparation for and response to significant cyber incidents. This effort will entail the following components:

- Mapping the current capabilities of government agencies related to cyber defense relative to detection and recognition of cyber activity of concern, attribution, response and mitigation, and reconstitution;
- Identifying capabilities within the government that US-CERT should leverage to maximize interagency coordination of cyber defense capabilities;
- Performing a gap analysis to identify the surge capabilities for possible leverage by or collaboration with the US-CERT for cyber defense issues in order to detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged; and
- Consider establishing formal resource sharing agreements with the other agencies per the cyber defense coordination needs identified through the process identified above.

Finally, NCSO has been supportive of the Department of Commerce's (DOC) efforts related to Internet Protocol version 6 (IPv6).⁵ The NCSO funded the IPv6 Task Force co-chaired by National Institute of Standards and Technology (NIST) and National Telecommunications and Information Administration (NTIA) in conducting an economic study of issues related to IPv6 deployment. The draft report, entitled "Technical and Economic Assessment of Internet Protocol Version 6 (IPv6)" opened for Federal Register comment in January 2005, and the DOC is holding a public meeting on July 28, 2005 to solicit additional input from stakeholders who may potentially be impacted by the report findings.

In addition, the US-CERT has released six technical bulletins and advisories pertaining to IPv6 regarding current vulnerabilities that exist and potential issues concerning deployment of IPv6. While the IPv6 standard has yet to be widely deployed, there exist several potential security risks that must be properly recognized and managed. These bulletins and advisories offer technical security recommendations for firewalls, configurations, cyber incident handling, and other relevant guidance for securing IPv6 enabled systems. DHS is supportive of OMB's efforts to facilitate the migration of federal agencies to IPV6 compatibility.

With our efforts, accomplishments, and on-going programs, NCSO has made significant progress in managing cyber incidents and has taken substantial strides toward building a National Cyberspace Response System; however, much remains to be done.

Priority 2 – Cyber Risk Management: Assessing the Threat and Reducing the Risk

⁵ The IP is a technical standard that enables computers and other devices to communicate with each other over networks, many of which interconnect to form the Internet. The current generation of IP, version 4 (IPv4) has been in use for more than 20 years. Through the guiding efforts of the Internet Engineering Task Force (IETF), a new version of IP, version 6, has been developed. Advantages of IPv6 over IPv4 include availability of more Internet addresses and additional user features and applications.

NCSD incorporated the risk management framework set out in HSPD-7 and the resulting interim NIPP into its effort to better assess the threats and reduce the vulnerabilities to our national cyberspace, and to mitigate and manage the consequences of a cyber attack. The NIPP Risk Management Framework entails a collaborative partnership among the private sector and federal, state, and local governments looking at people, cyber, and physical assets to identify and prioritize assets, assess vulnerabilities, and coordinate the protection of critical infrastructure and key resources.

With regard to assessing the risk, NCSD collaborates with the law enforcement and the intelligence communities in a number of ways. DHS assisted in the coordination of cyber-related issues for the "National Intelligence Estimate (NIE) of Cyber Threats to the U.S. Information Infrastructure." The resulting classified document issued in February 2004 details actors (nation states, terrorist groups, organized criminal groups, hackers, etc.), capabilities, and intent (where known). In addition, NCSD has infused cyber requirements into the Standing Information Needs (SINs) and Priority Information Needs (PINs) for the intelligence community and continues to collaborate with them through IA to characterize cyber threats for accuracy. Finally, the NCRCG includes law enforcement and intelligence agencies and has working groups addressing botnets and attribution issues.

There are four major components to NCSD's approach to reducing vulnerabilities. The central element of our approach is the cyber component of the NIPP. The other three key elements are the Internet Disruption Working Group (IDWG), the Control Systems Security Program, and the Software Assurance Program.

As I indicated, DHS is the SSA with NCSD as the lead for the Information Technology (IT) Sector and works with the Information Technology Information Sharing and Analysis Center (IT-ISAC) and the newly established Information Technology Sector Coordination Council (IT-SCC) supporting the NIPP framework. This public-private partnership is a crucial component of the NIPP framework, as more than 85 percent of the critical infrastructure is owned and operated by the private sector. In addition to its responsibility to work with the IT Sector to identify critical assets, assess vulnerabilities, and determine protective measures, NCSD is ensuring that cyber is comprehensive throughout the NIPP by providing guidance to the other critical infrastructure sectors in identifying, assessing, and protecting their cyber assets and cyber components of physical assets. This guidance includes contributing cyber elements to the NIPP Base Plan, reviewing the cyber aspects of Sector Specific Plans (SSPs), and delivering cyber CIP training to SSAs and SSP authors to help them enhance the cyber aspects of their SSPs, all of which are underway in NCSD.

Protection of critical cyber assets goes hand-in-hand with protection of critical telecommunications assets; accordingly, NCSD and NCS are working closely together to collaborate on issues related to threats, identification of critical cyber assets, vulnerability and risk assessments, and development of appropriate protective measures. Within the NIPP framework, NCSD and NCS established the Internet Disruption Working Group (IDWG) in December 2004 to address the resiliency and recovery of Internet functions in case of a major cyber incident. The Department of Treasury and the Department of Defense are also engaged, and the working group is acting to extend the partnership to representatives from the private

sector as well as international stakeholders. The IDWG reflects the convergence of telecommunications and information technology sectors in today's environment and the emergence of Next Generation Networks (NGN) that will compose the Internet of the future. An initial focus of the working group is to identify near term actions related to situational awareness, protection, and response that government and its stakeholders can take to better prepare for, protect against, and mitigate nationally significant Internet disruptions.

Future milestones for NCSD's CIP / Cyber Security Initiatives include efforts to:

- Develop IT Sector vulnerability assessment methodology and compile vulnerability assessment information;
- Define IT Sector specific metrics;
- Submit FY06 IT Sector Plan, subject to NIPP Council requirements;
- Compile FY06 IT Sector asset list and conduct FY06 asset prioritization; and,
- Develop, test, and publish cross-sector vulnerability assessment requirements as best practice.

The interdependency between physical and cyber infrastructures is hardly more acute than in the use of control systems as integral operating components by many of our critical infrastructures. "Control Systems" is a generic term applied to hardware, firmware, communications, and software used to perform vital monitoring and controlling functions of sensitive processes and enable automation of physical systems. Specific control systems used in the various critical infrastructure sectors include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems (PCS), and Distributed Control Systems (DCS).

Examples of the critical infrastructure processes and functions that control systems monitor and control include energy transmission and distribution, pipelines, water and pumping stations, chemical processing, pharmaceutical production, rail and light rail, manufacturing, and food production. Increasingly, these control systems are implemented with remote access, open connectivity, and connections to open networks such as corporate intranets and the Internet. These sophisticated information technology tools are making our critical infrastructure assets more automated, more productive, more efficient, and more innovative, but they also may expose many of those physical assets to physical consequences from new, cyber-related threats and vulnerabilities.

To assure immediate attention is directed to protect these systems, NCSD established the Control Systems Security Program to coordinate efforts among federal, state, and local governments, as well as control system owners, operators, and vendors to improve control system security within and across all critical infrastructure sectors. As part of this Program, NCSD developed a Control Systems Strategy that incorporates five highly integrated goals to address the issues and challenges associated with control systems security. As such, our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents, vulnerabilities, and mitigation of threat actions specific to critical control systems functions.

NCSD also established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other DOE National Laboratories⁶, the British Columbia Institute of Technology, and the private sector in June 2004. Since its establishment, the CSSC has made considerable progress and some of its major accomplishments include:

- Established the US-CERT CSSC assessment and incident response facility located at INL and a US-CERT Support Operations Center for Control Systems;
- Established relationships with more than 25 potential industry partners and completed several agreements that established initial assessment, analysis, and vulnerability reduction plans within various industry sectors;
- Created the Gross Consequence Matrix to determine the industries of most concern, and a list of specific sites from the National Asset Database where Control Systems could cause a negative consequence due to failure or attack;
- Created a quantitative control systems cyber risk/decision analysis measurement methodology; and,
- Established the Process Control System Forum (PCSF) (in partnership with DHS's Science and Technology Directorate) to accelerate the development of technology that will enhance the security, safety, and reliability of Control Systems, including legacy installations.

Future milestones for NCSD's Control Systems Security Program include efforts to:

- Develop a comprehensive set of control systems security assurance levels for owners and operators;
- Sponsor government/industry workshops to increase awareness among control systems owners and operators of potential cyber incident impacts and vulnerabilities;
- Develop, populate, and validate control systems security scenario assessment tools to provide response teams a web-based application to assess impacts;
- Assess a minimum of three core systems and provide solutions to vulnerabilities and recommendations to protect against cyber threats; and,
- Develop the US-CERT CSSC web page for information exchange.

The fourth major component of NCSD's cyber risk management program is our Software Assurance Program. Software is an essential component of the nation's critical infrastructure (power, water, transportation, financial institutions, defense industrial base, etc); however, defects in software can be exploited to launch cyber attacks as well as attacks against the critical infrastructure. NCSD developed a comprehensive software assurance framework that addresses people, process, technology, and acquisition throughout the software development lifecycle.

As part of the shared responsibility approach to cyber security, DHS is working to achieve a broader ability to routinely develop and deploy trustworthy software products. As such, DHS is shifting the security paradigm from "patch management" to "software assurance" by

⁶ Idaho (INL), Pacific Northwest (PNNL), Los Alamos (LANL), Argonne (ANL), Sandia (SNL), Savannah River (SRNL)

encouraging U.S. software developers to raise the bar on software quality and security. In collaboration with other federal agencies, academia, and the private sector, we are:

- Sponsoring the development of a repository of best practices and practical guidance for the software development community;
- Developing a software assurance common body of knowledge from which to develop curriculum for education and training;
- Facilitating discussions with industry and academic institutions through Software Assurance Forums (held in August 2004 and April 2005). The next forum is scheduled for October 2005;
- Collaborating with NIST to inventory software assurance tools and measure effectiveness, identify gaps and conflicts, and develop a plan to eliminate gaps and conflicts;
- Completing the DHS/Department of Defense co-sponsored comprehensive review of the National Information Assurance Partnership (NIAP)⁷ with the draft report to be published in September 2005; and
- Promoting investment in applicable software assurance research and development.

DHS will seek to reduce risks by raising the level of trust for all software, minimizing vulnerabilities and understanding threats. DHS will collaborate with government, industry, academic institutions, and international allies to achieve these software assurance objectives.

Moving Forward

We have studied the recent GAO report on critical infrastructure protection. We believe it has provided a fair assessment of the progress to date and agree that while considerable work has been done, much work remains to meet the challenges in this rapidly changing area. With the proposed appointment of a new Assistant Secretary for Cyber and Telecommunications Security, we are confident that we will accelerate our cyber security efforts.

Secretary Chertoff's recent release of the findings from his "Second Stage Review" of the entire Department illustrates DHS commitment to addressing leadership and organizational concerns that have been similarly raised by GAO.

We, tentatively, have identified three priority areas for collaboration with stakeholders that we will socialize with our public and private stakeholders in the next few weeks. These priority areas include information sharing, preparedness, and recovery. As part of that engagement, we will discuss our suggestion that the first priority should be to enhance preparedness collaboration by identifying the most significant cyber attack scenarios.

⁷ The National Information Assurance Partnership, established in August of 1997, is a joint effort between NIST and NSA to provide technical leadership in security-related information technology test methods and assurance techniques. NIAP uses the Common Criteria to evaluate and certify commercial off the shelf (COTS) products mainly for use by DoD and NSA. There has been much discussion in past years on the effectiveness (time and cost) of the NIAP process. As a result, the National Strategy to Secure Cyberspace recommended an independent review of the program be conducted to make recommendations for its improvement.

In connection with the interim National Infrastructure Protection Plan, we have begun our efforts to assess cyber threats and vulnerabilities, and identify significant interdependencies. These efforts will be fully implemented as the Sector Specific Agencies start implementing their portion of the NIPP. In partnership with NCS and other agencies we are working through the Internet Disruption Working Group to address the resiliency and recovery of internet functions in the case of a major cyber incident. We are working with the government, private sector, and academia to promote the integrity and security of software. We have planned a major exercise for later this year to test the Cyber Annex to the National Response Plan. Through this effort, we will pull together appropriate entities in the Federal government and appropriate private sector stakeholders to test our capabilities and, subsequently, to improve our incident management process.

We have also organized a Performance Metrics Team with internal representatives from all key substantive areas to ensure that each NCSD objective has associated metrics. We will seek private sector engagement in the development of metrics, including for cyber security preparedness. The Team will evaluate each objective to ensure the milestones and associated metrics are meaningful and capable of measuring performance and will develop measures to fulfill these needs.

We are committed to achieving success in meeting our goals and objectives, but we cannot do it alone. We will continue to meet with industry representatives, our government counterparts, academia, and state representatives to formulate the partnerships and leverage the efforts of all, so we, as a nation, are more secure in cyberspace.

Again, thank you for the opportunity to testify before you today. I would be glad to address you in the coming months on our progress and would now be pleased to answer any questions you have.

United States Government Accountability Office

GAO

Testimony before the Subcommittee on
Federal Financial Management, Government
Information, and International Security,
Senate Committee on Homeland Security and
Governmental Affairs

For Release on Delivery
Expected at 2:00 p.m. EDT
Tuesday, July 19, 2005

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Addressing Cybersecurity

Statement of David A. Powner,
Director, Information Technology
Management Issues



GAO-05-827T



Why GAO Did This Study

Increasing computer interconnectivity has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to our nation's computer systems and, more importantly, to the critical operations and infrastructures they support. The Homeland Security Act of 2002 and federal policy established the Department of Homeland Security (DHS) as the focal point for coordinating activities to protect the computer systems that support our nation's critical infrastructures. GAO was asked to summarize previous work, focusing on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection (CIP), (2) the status of the department's efforts to fulfill these responsibilities, (3) the challenges it faces in fulfilling its cybersecurity responsibilities, and (4) recommendations GAO has made to improve cybersecurity of our nation's critical infrastructure.

www.gao.gov/cgi-bin/gettrpt?GAO-05-827T

To view the full product, including the scope and methodology, click on the link above. For more information, contact David Pownier at (202) 512-9286 or pownierd@gao.gov.

July 2005

CRITICAL INFRASTRUCTURE PROTECTION

Challenges in Addressing Cybersecurity

What GAO Found

As the focal point for CIP, the Department of Homeland Security (DHS) has many cybersecurity-related roles and responsibilities that GAO identified in law and policy (see table below for 13 key responsibilities). DHS established the National Cyber Security Division to take the lead in addressing the cybersecurity of critical infrastructures.

While DHS has initiated multiple efforts to fulfill its responsibilities, it has not fully addressed any of the 13 responsibilities, and much work remains ahead. For example, the department established the United States Computer Emergency Readiness Team as a public/private partnership to make cybersecurity a coordinated national effort, and it established forums to build greater trust and information sharing among federal officials with information security responsibilities and law enforcement entities. However, DHS has not yet developed national cyber threat and vulnerability assessments or government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions.

DHS faces a number of challenges that have impeded its ability to fulfill its cybersecurity-related CIP responsibilities. These key challenges include achieving organizational stability, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders, and achieving two-way information sharing with these stakeholders. In its strategic plan for cybersecurity, DHS identifies steps that can begin to address the challenges. However, until it confronts and resolves these underlying challenges and implements its plans, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our critical infrastructures. In recent years, GAO has made a series of recommendations to enhance the cybersecurity of critical infrastructures that if effectively implemented could greatly improve our nation's cybersecurity posture.

Table: DHS's Key Cybersecurity Responsibilities

<ul style="list-style-type: none"> Develop a national plan for critical infrastructure protection, including cybersecurity. Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector. Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities. Develop and enhance national cyber analysis and warning capabilities. Provide and coordinate incident response and recovery planning efforts. 	<ul style="list-style-type: none"> Identify and assess cyber threats and vulnerabilities. Support efforts to reduce cyber threats and vulnerabilities. Promote and support research and development efforts to strengthen cyberspace security. Promote awareness and outreach. Foster training and certification. Enhance federal, state, and local government cybersecurity. Strengthen international cyberspace security. Integrate cybersecurity with national security.
--	---

Source: GAO analysis of law and policy.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing on challenges in protecting our nation's critical infrastructures from cybersecurity threats. Increasing computer interconnectivity—most notably growth in the use of the Internet—has revolutionized the way that our government, our nation, and much of the world communicate and conduct business. While the benefits have been enormous, this widespread interconnectivity also poses significant risks to the government's and our nation's computer systems and, more importantly, to the critical operations and infrastructures they support.

As requested, my testimony will focus on (1) DHS's responsibilities for cybersecurity-related critical infrastructure protection as established in law and policy, (2) the status of DHS's efforts to enhance the protection of the computer systems that support the nation's critical infrastructures and to strengthen information security—both inside and outside the federal government, (3) the challenges DHS faces in fulfilling its cybersecurity responsibilities, and (4) recommendations we have made to improve cybersecurity of national critical infrastructures. In preparing for this testimony, we relied on our previous work on critical infrastructure protection and cybersecurity threats; primarily on a recent report on the challenges faced by DHS in fulfilling its cybersecurity responsibilities.¹ All of the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

As the focal point for critical infrastructure protection, DHS has many cybersecurity-related responsibilities that are called for in law and policy. These responsibilities include developing plans, building

¹GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

partnerships, and improving information sharing, as well as implementing activities related to the five priorities in the national cyberspace strategy: (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. To fulfill its cybersecurity role, in June 2003, the department established the National Cyber Security Division to serve as a national focal point for addressing cybersecurity and coordinating the implementation of cybersecurity efforts.

While DHS has initiated multiple efforts, it has not fully addressed any of the 13 key cybersecurity-related responsibilities that we identified in federal law and policy, and it has much work ahead in order to be able to fully address them. For example, DHS (1) has recently issued the *Interim National Infrastructure Protection Plan*, which includes cybersecurity elements; (2) operates the United States Computer Emergency Readiness Team to address the need for a national analysis and warning capability; and (3) has established forums to foster information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed national threat and vulnerability assessments or developed and exercised government and government/industry contingency recovery plans for cybersecurity, including a plan for recovering key Internet functions. Further, DHS continues to have difficulties in developing partnerships—as called for in federal policy—with other federal agencies, state and local governments, and the private sector.

DHS faces a number of challenges that have impeded its ability to fulfill its cyber-related critical infrastructure protection (CIP) responsibilities. Key challenges include achieving organizational stability; gaining organizational authority; overcoming hiring and contracting issues; increasing awareness about cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal agencies, state and local governments and the private sector); achieving two-way information sharing with these stakeholders; and demonstrating the value it can provide. In

its strategic plan for cybersecurity, the department has identified steps that can begin to address these challenges. However, until it effectively confronts and resolves these underlying challenges, DHS will have difficulty achieving significant results in strengthening the cybersecurity of our nation's critical infrastructures, and our nation will lack the strong cybersecurity focal point envisioned in federal law and policy.

Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures, focusing on the need to (1) develop a strategic analysis and warning capability for identifying potential cyberattacks, (2) protect infrastructure control systems, (3) enhance public/private information sharing, and (4) conduct important threat and vulnerability assessments and address other challenges to effective cybersecurity. Effectively implementing these recommendations could greatly improve our nation's cybersecurity posture.

Background

The same speed and accessibility that create the enormous benefits of the computer age can, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with computer operations from remote locations for mischievous or malicious purposes, including fraud or sabotage. In recent years, the sophistication and effectiveness of cyberattacks have steadily advanced. These attacks often take advantage of flaws in software code, circumvent signature-based tools² that commonly identify and prevent known threats, and use social engineering techniques designed to trick the unsuspecting user into divulging sensitive information or propagating attacks. These attacks are becoming increasingly automated with the use of botnets—compromised computers that can be remotely controlled by attackers to automatically launch attacks. Bots (short for robots)

² Signature-based tools compare files or packets to a list of "signatures"—patterns of specific files or packets that have been identified as threats.

have become a key automation tool used to speed the infection of vulnerable systems.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence-gathering, and acts of war. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

Recent attacks and threats have further underscored the need to bolster the cybersecurity of our government's and our nation's computer systems and, more importantly, of the critical operations and infrastructures they support. Recent examples of attacks include the following:

- In March 2005, security consultants within the electric industry reported that hackers were targeting the U.S. electric power grid and had gained access to U.S. utilities' electronic control systems. Computer security specialists reported that, in a few cases, these intrusions had "caused an impact." While officials stated that hackers had not caused serious damage to the systems that feed the nation's power grid, the constant threat of intrusion has heightened concerns that electric companies may not have adequately fortified their defenses against a potential catastrophic strike.
- In January 2005, a major university reported that a hacker had broken into a database containing 32,000 student and employee Social Security numbers, potentially compromising their identities and finances. In similar incidents during 2003 and 2004, it was reported that hackers had attacked the systems of other universities, exposing the personal information of over 1.8 million people.
- In June 2003, the U.S. government issued a warning concerning a virus that specifically targeted financial institutions. Experts said the BugBear.b virus was programmed to determine whether a victim had used an e-mail address for any of the roughly 1,300

financial institutions listed in the virus's code. If a match was found, the software attempted to collect and document user input by logging keystrokes and then provided this information to a hacker, who could use it in attempts to break into the banks' networks.

- In November 2002, a British computer administrator was indicted on charges that he accessed and damaged 98 computers in 14 states between March 2001 and March 2002, causing some \$900,000 in damage. These networks belonged to the Department of Defense, the National Aeronautics and Space Administration, and private companies. The indictment alleges that the attacker was able to gain administrative privileges on military computers, copy password files, and delete critical system files. The attacks rendered the networks of the Earle Naval Weapons Station in New Jersey and the Military District of Washington inoperable.

In May 2005, we reported that federal agencies are facing a set of emerging cybersecurity threats that are the result of increasingly sophisticated methods of attack and the blending of once distinct types of attack into more complex and damaging forms.³ Examples of these threats include *spam* (unsolicited commercial e-mail), *phishing* (fraudulent messages used to obtain personal or sensitive data), and *spyware* (software that monitors user activity without the user's knowledge or consent). Spam consumes significant resources and is used as a delivery mechanism for other types of cyberattacks; phishing can lead to identity theft, loss of sensitive information, and reduced trust and use of electronic government services; and spyware can capture and release sensitive data, make unauthorized changes, and decrease system performance.

³ GAO, *Information Security: Emerging Cybersecurity Issues Threaten Federal Information Systems*, GAO-05-231 (Washington, D.C.: May 13, 2005).

DHS's Responsibilities for Cybersecurity in Support of Critical Infrastructure Protection Are Many and Varied

Federal law and policies call for critical infrastructure protection (CIP) activities that are intended to enhance the cyber and physical security of both the public and private infrastructures that are essential to national security, national economic security, and national public health and safety.⁴ Federal policy designates certain federal agencies as lead federal points of contact for the critical infrastructure sectors and assigns them responsibility for infrastructure protection activities in their assigned sectors and for coordination with other relevant federal agencies, state and local governments, and the private sector to carry out related responsibilities (see app. 1). In addition, federal policy establishes the Department of Homeland Security (DHS) as the focal point for the security of cyberspace—including analysis, warning, information sharing, vulnerability reduction, mitigation, and recovery efforts for public and private critical infrastructure information systems. To accomplish this mission, DHS is to work with other federal agencies, state and local governments, and the private sector.

Among the many CIP responsibilities established for DHS and identified in federal law and policy are 13 key cybersecurity-related responsibilities. These include general CIP responsibilities that have a cyber element (such as developing national plans, building partnerships, and improving information sharing) as well as responsibilities that relate to the five priorities established by the *National Strategy to Secure Cyberspace*. The five priorities are (1) developing and enhancing national cyber analysis and warning, (2) reducing cyberspace threats and vulnerabilities, (3) promoting awareness of and training in security issues, (4) securing governments' cyberspace, and (5) strengthening national security and international cyberspace security cooperation. Table 1 provides a description of each of these responsibilities.

⁴This law and these policies include the Homeland Security Act of 2002, Homeland Security Presidential Directive 7, and the *National Strategy to Secure Cyberspace*.

Table 1: Thirteen DHS Cybersecurity Responsibilities

General CIP responsibilities with a cyber element	Description
Develop a national plan for critical infrastructure protection that includes cybersecurity.	Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States, including information technology and telecommunications systems (including satellites) and the physical and technological assets that support such systems. This plan is to outline national strategies, activities, and milestones for protecting critical infrastructures.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	Fostering and developing public/private partnerships with and among other federal agencies, state and local governments, the private sector, and others. DHS is to serve as the "focal point for the security of cyberspace."
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	Improving and enhancing information sharing with and among other federal agencies, state and local governments, the private sector, and others through improved partnerships and collaboration, including encouraging information sharing and analysis mechanisms. DHS is to improve sharing of information on cyber attacks, threats, and vulnerabilities.
Responsibilities related to the cyberspace strategy's five priorities	
Develop and enhance national cyber analysis and warning capabilities.	Providing cyber analysis and warnings, enhancing analytical capabilities, and developing a national indications and warnings architecture to identify precursors to attacks.
Provide and coordinate incident response and recovery planning efforts.	Providing crisis management in response to threats to or attacks on critical information systems. This entails coordinating efforts for incident response, recovery planning, exercising cybersecurity continuity plans for federal systems, planning for recovery of Internet functions, and assisting infrastructure stakeholders with cyber-related emergency recovery plans.
Identify and assess cyber threats and vulnerabilities.	Leading efforts by the public and private sector to conduct a national cyber threat assessment, to conduct or facilitate vulnerability assessments of sectors, and to identify cross-sector interdependencies.
Support efforts to reduce cyber threats and vulnerabilities.	Leading and supporting efforts by the public and private sector to reduce threats and vulnerabilities. Threat reduction involves working with law enforcement community to investigate and prosecute cyberspace threats. Vulnerability reduction involves identifying and remediating vulnerabilities in existing software and systems.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborating and coordinating with members of academia, industry, and government to optimize cybersecurity related research and development efforts to reduce vulnerabilities through the adoption of more secure technologies.
Promote awareness and outreach.	Establishing a comprehensive national awareness program to promote efforts to strengthen cybersecurity throughout government and the private sector, including the home user.
Foster training and certification.	Improving cybersecurity-related education, training, and certification opportunities.
Enhance federal, state, and local government cybersecurity.	Partnering with federal, state, and local governments in efforts to strengthen the cybersecurity of the nation's critical information infrastructure to assist in the deterrence, prevention, preemption of, and response to terrorist attacks against the United States.
Strengthen international cyberspace security.	Working in conjunction with other federal agencies, international organizations, and industry in efforts to promote strengthened cybersecurity on a global basis.
Integrate cybersecurity with national security.	Coordinating and integrating applicable national preparedness goals with its National Infrastructure Protection Plan.

Source: GAO analysis of the Homeland Security Act of 2002, the Homeland Security Presidential Directive-7, and the National Strategy to Secure Cyberspace.

In June 2003, DHS established the National Cyber Security Division (NCSD), under its Information Analysis and Infrastructure Protection Directorate, to serve as a national focal point for addressing cybersecurity issues and to coordinate implementation of the cybersecurity strategy. NCSD also serves as the government lead on a public/private partnership supporting the U.S. Computer Emergency Response Team (US-CERT) and as the lead for federal government incident response. NCSD is headed by the Office of the Director and includes a cybersecurity partnership program as well as four branches: US-CERT Operations, Law Enforcement and Intelligence, Outreach and Awareness, and Strategic Initiatives.

DHS Has Initiated Efforts That Begin to Address Its Responsibilities, but More Work Remains

DHS has initiated efforts that begin to address each of its 13 key responsibilities for cybersecurity; however, the extent of progress varies among these responsibilities, and more work remains to be done on each. For example, DHS (1) has recently issued an interim plan for infrastructure protection that includes cybersecurity plans, (2) is supporting a national cyber analysis and warning capability through its role in US-CERT, and (3) has established forums to build greater trust and to encourage information sharing among federal officials with information security responsibilities and among various law enforcement entities. However, DHS has not yet developed a national cyber threat assessment and sector vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy. The importance of such assessments is illustrated in our recent reports on vulnerabilities in infrastructure control systems and in wireless networks.³ Further, the department has not yet developed and exercised government and government/industry contingency

³GAO, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems*, GAO-04-354, (Washington, D.C.: Mar. 15, 2004) and *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*, GAO-05-333, (Washington, D.C.: May 17, 2005).

recovery plans for cybersecurity, including a plan for recovering key Internet functions. The department also continues to have difficulties in developing partnerships, as called for in federal policy, with other federal agencies, state and local governments, and the private sector. Without such partnerships, it is difficult to develop the trusted, two-way information sharing that is essential to improving homeland security.

Table 2 provides an overview of the steps that DHS has taken related to each of its 13 key responsibilities and identifies the steps that remain.

Table 2: Overview of Progress and Remaining Activities on DHS's 13 Cybersecurity-related Responsibilities

DHS Responsibility	DHS Progress	Status/What Remains
Develop a national plan for critical infrastructure protection that includes cybersecurity.	Issued Interim National Infrastructure Protection Plan that includes cybersecurity-related initiatives	The plan is not yet comprehensive and complete. DHS plans to add sector-specific cybersecurity details and milestones in subsequent versions.
Develop partnerships and coordinate with other federal agencies, state and local governments, and the private sector.	Undertook numerous initiatives to foster partnerships and enhance information sharing with other federal agencies, state and local governments, and the private sector about cyber attacks, threats, and vulnerabilities.	Information sharing has been limited. More work is needed to address barriers to effective partnerships and information sharing.
Improve and enhance public/private information sharing involving cyber attacks, threats, and vulnerabilities.	Initiatives include the National Cyber Security Response System and Information Sharing and Analysis Center (ISAC) partnerships.	
Develop and enhance national cyber analysis and warning capabilities.	Provides cyber analysis and warning capabilities through continuous operational support of the US-CERT; is working to enhance tools and communication mechanisms for providing analysis and warning of potential cyber incidents.	Efforts are not complete. DHS has not yet developed the indications and warning architecture required by HSPD-7, and important analytical tools are not yet mature.
Provide and coordinate incident response and recovery planning efforts.	Improved ability to coordinate a response to cyber attacks with federal, state, and local governments and private-sector entities through the communications capabilities developed for US-CERT, continued expansion of backup communication capabilities, and establishment of collaboration mechanisms.	Plans and exercises for recovering from attacks are not yet complete and comprehensive. DHS does not yet have plans for testing federal continuity plans, recovering key Internet functions, or providing technical assistance to both private-sector and other government entities as they develop their own emergency recovery plans.
Identify and assess cyber threats and vulnerabilities.	Participated in national efforts to identify and assess cyber threats and has begun taking steps to facilitate sector-specific vulnerability assessments	Assessments are not yet complete. DHS has not yet completed the comprehensive cyber threat and vulnerability assessments—or the identification of cross-sector interdependencies—that are called for in the cyberspace strategy.

Support efforts to reduce cyber threats and vulnerabilities.	Initiated efforts to reduce threats by enhancing collaboration with the law enforcement community and to reduce vulnerabilities by shoring up guidance on software and system security.	Efforts are not complete. Vulnerability reduction efforts are limited until the cyber-related vulnerability assessments (discussed in the previous section) are completed.
Promote and support research and development efforts to strengthen cyberspace security.	Collaborated with the Executive Office of the President and with other federal departments and agencies to develop a national research and development plan for CIP, including cybersecurity.	A comprehensive plan is not yet in place, and the milestones for key activities have not yet been established. The stakeholders expect to issue a plan with a roadmap, investment plan, and milestones next year.
Promote awareness and outreach.	Made progress in increasing cybersecurity awareness by implementing numerous awareness and outreach initiatives, including the National Cyber Alert System, the National Cyber Security Awareness Month program, and the US CERT public Web site.	The effectiveness of awareness and outreach activities is unclear. Many CIP stakeholders are still uncertain of DHS's cybersecurity roles.
Foster training and certification.	Initiated multiple efforts to improve the education of future cybersecurity analysts, including cosponsoring the National Centers of Academic Excellence in Information Assurance program and fostering the scholarship for service program.	Efforts are not yet complete. Much work remains to be done to develop certification standards.
Enhance federal, state, and local government cybersecurity.	Supports multiple interagency groups' efforts to improve government cybersecurity, including the Chief Information Security Officers forum, the National Cyber Response Coordination Group, and the Government Forum of Incident Response and Security Teams.	Efforts are not yet complete. State and local government stakeholders have expressed concerns about the scope of these efforts.
Strengthen international cyberspace security.	Works in conjunction with other foreign governments to promote a global culture of security. Initiatives include participation in the G-8 High Tech Crime working group and the International Watch and Warning Framework/Multilateral Conference.	More remains to be done. DHS plans to create and pursue an international strategy to secure cyberspace and to promote collaboration, coordination, and information sharing with international communities.
Integrate cybersecurity with national security.	Formed the National Cyber Response Coordinating Group—a forum of national security, law enforcement, defense, intelligence, and other government agencies—that coordinates intragovernmental and public/private preparedness and response to and recovery from national-level cyber incidents and physical attacks that have significant cyber consequences.	Important testing remains to be done. Early tests of this coordination showed the need to improve communication protocols; additional testing is warranted.

Source: GAO analysis of DHS information.

DHS Continues to Face Challenges in Establishing Itself as a National Focal Point for Cyberspace Security

DHS faces a number of challenges that have impeded its ability to fulfill its cyber CIP responsibilities. Key challenges include achieving organizational stability, gaining organizational authority, overcoming hiring and contracting issues, increasing awareness about cybersecurity roles and capabilities, establishing effective partnerships with stakeholders (other federal, state, and local governments and the private sector), achieving two-way information sharing with these stakeholders, and providing and demonstrating the value DHS can provide.

Organizational stability: Over the last year, multiple senior DHS cybersecurity officials—including the NCSD Director, the Deputy Director responsible for Outreach and Awareness, and the Director of the US-CERT Control Systems Security Center, the Under Secretary for the Information Analysis and Infrastructure Protection Directorate and the Assistant Secretary responsible for the Information Protection Office—have left the department. Infrastructure sector officials stated that the lack of stable leadership has diminished NCSD's ability to maintain trusted relationships with its infrastructure partners and has hindered its ability to adequately plan and execute activities. According to one private-sector representative, the importance of organizational stability in fostering strong partnerships cannot be over emphasized.

Organizational authority: NCSD does not have the organizational authority it needs to effectively serve as a national focal point for cybersecurity. Accordingly, its officials lack the authority to represent and commit DHS to efforts with the private sector. Infrastructure and cybersecurity officials, including the chairman of the sector coordinators and representatives of the cybersecurity industry, have expressed concern that the cybersecurity division's relatively low position within the DHS organization hinders its ability to accomplish cybersecurity-related goals. NCSD's lack of authority has led to some missteps, including DHS's cancellation of an important cyber event without explanation and its taking almost a year to issue formal responses to private sector recommendations.

that resulted from selected National Cyber Security Summit task forces—even though responses were drafted within months.

A congressional subcommittee also expressed concern that DHS's cybersecurity office lacks the authority to effectively fulfill its role. In 2004 and again in 2005, the subcommittee proposed legislation to elevate the head of the cybersecurity office to an assistant secretary position. Among other benefits, the subcommittee reported that such a change could

- provide more focus and authority for DHS's cybersecurity mission,
- allow higher level input into national policy decisions, and
- provide a single visible point of contact within the federal government for improving interactions with the private sector.

Hiring and contracting: Ineffective DHS management processes have impeded the department's ability to hire employees and maintain contracts. We recently reported that since DHS's inception, its leadership has provided a foundation for maintaining critical operations while it undergoes transformation.⁶ However, in managing its transformation, we noted that the department still needed to overcome a number of significant challenges, including addressing systemic problems in human capital and acquisition systems. Federal and nonfederal officials expressed concerns about its hiring and contracting processes. For example, an NCSD official reported that the division has had difficulty in hiring personnel to fill vacant positions. These officials stated that once they found qualified candidates, some candidates decided not to apply and another one withdrew his acceptance because he felt that DHS's hiring process had taken too long. In addition, a cybersecurity division official stated that there had been times when DHS did not renew NCSD contracts in a timely manner, requiring that key contractors work without pay until approvals could be completed and payments could be made. In other cases, NCSD was denied services from a vendor because the department had repeatedly

⁶GAO, *High-Risk Series: An Update*, GAO-05-207, (Washington, D.C.: January, 2005).

failed to pay this vendor for its services. External stakeholders, including an ISAC representative, also noted that NCSD is hampered by how long it takes DHS to award a contract.

Awareness of DHS roles and capabilities: Many infrastructure stakeholders are not yet aware of DHS's cybersecurity roles and capabilities. Department of Energy critical infrastructure officials stated that the roles and responsibilities of DHS and the sector-specific agencies need to be better clarified in order to improve coordination. In addition, during a regional cyber exercise, private-sector and state and local government officials reported that the mission of NCSD and the capabilities that DHS could provide during a serious cyber-threat were not clear to them. NCSD's manager of cyber analysis and warning operations acknowledged that the organization has not done an adequate job reaching out to the private sector regarding the department's role and capabilities.

Effective partnerships: NCSD is responsible for leveraging the assets of key stakeholders, including other federal, state, and local governments and the private sector, in order to facilitate effective protection of cyber assets. The ability to develop partnerships greatly enhances the agency's ability to identify, assess, and reduce cyber threats and vulnerabilities, establish strategic analytical capabilities, provide incident response, enhance government cybersecurity, and improve international efforts. According to one infrastructure sector representative, effective partnerships require building relationships with mutually developed goals; shared benefits and responsibilities; and tangible, measurable results. However, this individual reported that DHS has not typically adopted these principles in pursuing partnerships with the private sector, which dramatically diminishes cybersecurity gains that government and industry could otherwise achieve. For example, it has often informed the infrastructure sectors about government initiatives or sought input after most key decisions have been made. Also, the department has not demonstrated that it recognizes the value of leveraging existing private sector mechanisms, such as information-sharing entities and processes that are already in place and working. In addition, the instability of NCSD's leadership positions to date has led to problems in developing partnerships. Representatives from two ISACs reported that turnover at the

cybersecurity division has hindered partnership efforts. Additionally, IT sector representatives stated that NCSD needs continuity of leadership, regular communications, and trusted policies and procedures in order to build the partnerships that will allow the private sector to share information.

Information sharing: We recently identified information sharing in support of homeland security as a high-risk area, and we noted that establishing an effective two-way exchange of information to help detect, prevent, and mitigate potential terrorist attacks requires an extraordinary level of cooperation and perseverance among federal, state, and local governments and the private sector.⁷ However, such effective communications are not yet in place in support of our nation's cybersecurity. Representatives from critical infrastructure sectors stated that entities within their respective sectors still do not openly share cybersecurity information with DHS. As we have reported in the past, much of the concern is that the potential release of sensitive information could increase the threat to an entity. In addition, sector representatives stated that when information is shared, it is not clear whether the information will be shared with other entities—such as other federal entities, state and local entities, law enforcement, or various regulators—and how it will be used or protected from disclosure. Representatives from the banking and finance sector stated that the protection provided by the Critical Infrastructure Information Act and the subsequently established Protected Critical Infrastructure Information Program is not clear and has not overcome the trust barrier. Sector representatives have expressed concerns that DHS is not effectively communicating information to them. According to one infrastructure representative, DHS has not matched private sector efforts to share valuable information with a corresponding level of trusted information sharing. An official from the water sector noted that when representatives called DHS to inquire about a potential terrorist threat, they were told that DHS could not share any information and that they should “watch the news.”

⁷GAO-05-207.

Providing value: According to sector representatives, even when organizations within their sectors have shared information with NCSD, the entities do not consistently receive useful information in return. They noted that without a clear benefit, they are unlikely to pursue further information sharing with DHS. Federal officials also noted problems in identifying the value that DHS provides. According to Department of Energy officials, the department does not always provide analysis or reports based on the information that agencies provide. Federal and nonfederal officials also stated that most of US-CERT's alerts have not been useful because they lack essential details or are based on already available information. Further, Treasury officials stated that US-CERT needed to provide relevant and timely feedback regarding the incidents that are reported to it.

Clearly, these challenges are not mutually exclusive. That is, addressing challenges in organizational stability and authority will help NCSD build the credibility it needs in order to establish effective partnerships and achieve two-way information sharing. Similarly, effective partnerships and ongoing information sharing with its stakeholders will allow DHS to better demonstrate the value it can add.

DHS has identified steps in its strategic plan for cybersecurity that can begin to address these challenges. Specifically, it has established goals and plans for improving human capital management that should help stabilize the organization. Further, the department has developed plans for communicating with stakeholders that are intended to increase awareness of its roles and capabilities and to encourage information sharing. Also, it has established plans for developing effective partnerships and improving analytical and watch and warning capabilities that could help build partnerships and begin to demonstrate added value. However, until it begins to address these underlying challenges, DHS cannot achieve significant results in coordinating cybersecurity activities, and our nation will lack the effective focal point it needs to better ensure the security of cyberspace for public and private critical infrastructure systems.

Implementation of GAO Recommendations Should Enhance Cybersecurity of Critical Infrastructures

Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures, focusing on the need to (1) develop a strategic analysis and warning capability for identifying potential cyberattacks, (2) protect infrastructure control systems, (3) enhance public/private information sharing, and (4) conduct important threat and vulnerability assessments and address other challenges to effective cybersecurity. These recommendations are summarized below.

Strategic Analysis and Warnings: In 2001, we reported on the analysis and warnings efforts within DHS's predecessor, the National Infrastructure Protection Center, and identified several challenges that were impeding the development of an effective strategic analysis and warning capability.⁸ We reported that a generally accepted methodology for analyzing strategic cyber-based threats did not exist. Specifically, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. We also reported that the Center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies.

We therefore recommended that the responsible executive-branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data. However, officials have taken little action to establish this capability, and therefore our recommendations remain open today.

⁸GAO, *Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities*, GAO-01-323 (Washington, D.C.: Apr. 25, 2001).

Control Systems: In March 2004, we reported that several factors—including the adoption of standardized technologies with known vulnerabilities and the increased connectivity of control systems to other systems—contributed to an escalation of the risk of cyber-attacks against control systems.⁹ We recommended that DHS develop and implement a strategy for coordinating with the private sector and with other government agencies to improve control system security, including an approach for coordinating the various ongoing efforts to secure control systems. DHS concurred with our recommendation and, in December 2004, issued a high-level national strategy for control systems security. This strategy includes, among other things, goals to create a capability to respond to attacks on control systems and to mitigate vulnerabilities, bridge industry and government efforts, and develop control systems security awareness. However, the strategy does not yet include underlying details and milestones for completing activities.

Information Sharing: In July 2004, we recommended actions to improve the effectiveness of DHS's information-sharing efforts.¹⁰ We recommended that officials within the Information Analysis and Infrastructure Protection Directorate (1) proceed with and establish milestones for developing an information-sharing plan and (2) develop appropriate DHS policies and procedures for interacting with ISACs, sector coordinators (groups or individuals designated to represent their respective infrastructure sectors' CIP activities), and sector-specific agencies and for coordination and information sharing within the Information Analysis and Infrastructure Protection Directorate and other DHS components. These recommendations remain open today. Moreover, we recently designated establishing appropriate and effective information-sharing mechanisms to improve homeland security as a new high-risk area.¹¹ We reported that the ability to share security-related information can unify the efforts of federal, state, and local

⁹ GAO-04-354.

¹⁰ GAO, *Critical Infrastructure Protection: Improving Information Sharing with Infrastructure Sectors*, GAO-04-790 (Washington, D.C.: July 9, 2004).

¹¹ GAO-05-207.

government agencies and the private sector in preventing or minimizing terrorist attacks.

Threat and Vulnerability Assessments and Other Challenges:

Most recently, in May 2005, we reported that while DHS has made progress in planning and coordinating efforts to enhance cybersecurity, much more work remains to be done to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments and recovery plans. Further, we reported that DHS faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private/public assets and information in order to clearly demonstrate the value it can provide. We made recommendations to strengthen the department's ability to implement key cybersecurity responsibilities by prioritizing and completing critical activities and resolving underlying challenges.

We recently met with DHS's acting director for cybersecurity who told us that DHS agreed with our findings and has initiated plans to address our recommendations. He acknowledged that DHS has not adequately leveraged their public and private stakeholders in a prioritized manner and it plans to begin its prioritized approach by focusing stakeholders on information sharing, preparedness, and recovery. He also added that the next iteration of the *National Infrastructure Protection Plan* will focus on Internet recovery, control systems, and software assurance.

In summary, as our nation has become increasingly dependent on timely, reliable information, it has also become increasingly vulnerable to attacks on the information infrastructure that supports the nation's critical infrastructures (including the energy, banking and finance, transportation, telecommunications, and drinking water infrastructures). Federal law and policy acknowledge this by establishing DHS as the focal point for coordinating cybersecurity plans and initiatives with other federal agencies, state and local

governments, and private industry. DHS has made progress in planning and coordinating efforts to enhance cybersecurity, but much more work remains to be done for the department to fulfill its basic responsibilities—including conducting important threat and vulnerability assessments and recovery plans.

As DHS strives to fulfill its mission, it faces key challenges in building its credibility as a stable, authoritative, and capable organization and in leveraging private and public assets and information in order to clearly demonstrate the value it can provide. Until it overcomes the many challenges it faces and completes critical activities, DHS cannot effectively function as the cybersecurity focal point intended by law and national policy. As such, there is increased risk that large portions of our national infrastructure are either unaware of key areas of cybersecurity risks or unprepared to effectively address cyber emergencies. Over the last several years, we have made a series of recommendations to enhance the cybersecurity of critical infrastructures. These include (1) developing a strategic analysis and warning capability for identifying potential cyberattacks, (2) protecting infrastructure control systems, (3) enhancing public/private information sharing, and (4) conducting important threat and vulnerability assessments and address other challenges to effective cybersecurity. Effectively implementing these recommendations could greatly improve our nation's cybersecurity posture.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-9286 or by e-mail at pownerd@gao.gov. Other key contributors to this report include Joanne Florino, Michael Gilmore, Barbarol James, Colleen Phillips, and Nik Rapelje.

Appendix I: Infrastructure Sectors and Lead Agencies Identified by Federal Policies on Critical Infrastructure Protection

Sector	Description	Lead agency
Agriculture	Provides for the fundamental need for food. The infrastructure includes supply chains for feed and crop production.	Department of Agriculture
Banking and finance	Provides the financial infrastructure of the nation. This sector consists of commercial banks, insurance companies, mutual funds, government-sponsored enterprises, pension funds, and other financial institutions that carry out transactions, including clearing and settlement.	Department of the Treasury
Chemicals and hazardous materials	Transforms natural raw materials into commonly used products benefiting society's health, safety, and productivity. The chemical industry produces more than 70,000 products that are essential to automobiles, pharmaceuticals, food supply, electronics, water treatment, health, construction, and other necessities.	Department of Homeland Security
Commercial facilities	Includes prominent commercial centers, office buildings, sports stadiums, theme parks, and other sites where large numbers of people congregate to pursue business activities, conduct personal commercial transactions, or enjoy recreational pastimes.	Department of Homeland Security
Dams	Comprises approximately 80,000 dam facilities, including larger and nationally symbolic dams that are major components of other critical infrastructures that provide electricity and water.	Department of Homeland Security
Defense industrial base	Supplies the military with the means to protect the nation by producing weapons, aircraft, and ships and providing essential services, including information technology and supply and maintenance.	Department of Defense
Drinking water and water treatment systems	Sanitizes the water supply through about 170,000 public water systems. These systems depend on reservoirs, dams, wells, treatment facilities, pumping stations, and transmission lines.	Environmental Protection Agency
Emergency services	Saves lives and property from accidents and disaster. This sector includes fire, rescue, emergency medical services, and law enforcement organizations.	Department of Homeland Security
Energy	Provides the electric power used by all sectors, including critical infrastructures, and the refining, storage, and distribution of oil and gas. The sector is divided into electricity and oil and natural gas.	Department of Energy
Food	Carries out the post-harvesting of the food supply, including processing and retail sales.	Department of Agriculture and Department of Health and Human Services
Government	Ensures national security and freedom and administers key public functions.	Department of Homeland Security
Government facilities	Includes the buildings owned and leased by the federal government for use by federal entities.	Department of Homeland Security
Information technology and telecommunications	Provides communications and processes to meet the needs of businesses and government.	Department of Homeland Security

Sector	Description	Lead agency
National monuments and icons	Includes key assets that are symbolically equated with traditional American values and institutions or U.S. political and economic power.	Department of the Interior
Nuclear reactors, materials, and waste	Includes 104 commercial nuclear reactors; research and test nuclear reactors; nuclear materials; and the transportation, storage, and disposal of nuclear materials and waste.	Department of Homeland Security working with the Nuclear Regulatory Agency and Department of Energy
Postal and shipping	Delivers private and commercial letters, packages, and bulk assets. The U.S. Postal Service and other carriers provide the services of this sector.	Department of Homeland Security
Public health and healthcare	Mitigates the risk of disasters and attacks and also provides recovery assistance if an attack occurs. The sector consists of health departments, clinics, and hospitals.	Department of Health and Human Services
Transportation systems	Enables movement of people and of assets that are vital to our economy, mobility, and security via aviation, ships, rail, pipelines, highways, trucks, buses, and mass transit.	Department of Homeland Security in collaboration with the Department of Transportation

Source: GAO analysis based on the President's National Strategy documents and HSPD-7.

69

Testimony by

Paul Skare

Product Manager

Siemens Power Transmission & Distribution, Inc.

Energy Management & Automation

to the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management, Government

Information, and International Security

July 19, 2005

Introduction

Good afternoon Chairman Coburn, ranking member Carper, and members of the Subcommittee on Federal Financial Management, Government Information, and International Security. I am Paul Skare, Product Manager at Siemens Power, Transmission and Distribution, Inc. I am representing one of the manufacturers of SCADA (Supervisory Control and Data Acquisition) systems. My role at Siemens includes managing products for SCADA systems as well as substation automation systems. I am also involved in standards groups related to SCADA.

Siemens is one of the largest electronics companies in the world, operating in over 190 countries. We're a diversified company, delivering a wide array of products, systems and services in six main industries. These include information and communications, automation and control, power, healthcare, transportation and lighting. Siemens has over 70,000 employees in the United States across all 50 states.

Siemens' Energy Management & Automation provides software and technologies in regulated and deregulated energy markets. A key product for these markets is SCADA. SCADA collects information from devices in the power system, identifies problems, and allows users to remotely control these devices. Adding additional applications to a SCADA allows a more focused and enhanced solution for transmission or distribution systems (referred to as an Energy Management System (EMS) for transmission or a Distribution Management System (DMS) for

distribution).

My testimony today focuses on identifying potential security vulnerabilities of SCADA systems, the state of activities related to this, and recommendations to better protect those systems from harmful intrusion.

While our customers primarily use our SCADA systems for the electric system, some also use the same SCADA system for gas, water, and transportation systems. Although our systems are not used as commonly in other settings such as industrial control systems, the concepts are the same across all SCADA systems. In the appendixes of the written testimony, I have provided background information on SCADA and security issues relevant to SCADA. I would like to take this opportunity to congratulate the industry and the government in the work that has been done in the last three years in this area – it has started moving this work from the realm of art to science, and is finally starting to not only spread awareness, but also to get various players to talk the same language.

SCADA Vulnerabilities

SCADA vulnerabilities that may be a problem often involve issues associated with the following:

Remote Access

Remote access to SCADA systems is available for a variety of reasons: user access

outside of the control room, user support, and vendor support. This is a problem if there are any accidental (configuration of) security holes. If any backdoors are in the system (either leftover from the vendor or in place for user support), access points are easier to exploit. Local access points must be physically secure or these issues will also apply to them.

Network configurations

Network (and firewall) configurations are a very important aspect for SCADA systems. SCADA systems depend on a network for operational needs. If a firewall is bypassed accidentally or is miss-configured, a severe security hole could exist.

Disgruntled employees

If an employee becomes disgruntled, either before or after action by a utility (current or former employees), if the security process has not yet closed all access for that individual, the case for doing damage is greatest, since all the security in place can still be used by an authorized individual.

Security holes, patches, viruses

Systems rely on standard IT solutions [Commercial Off The Shelf (COTS)] to create a SCADA solution. Some third party security holes in operating systems, commercial databases and other applications can directly translate into security issues for the SCADA.

Communication protocols not encrypted

Communications, being the largest cost driver in a SCADA solution, is an important area. Since many field devices can last 30 or more years, utilities are reluctant to upgrade them unless there are clear needs. This means many old low power (computationally) devices are in operation, for which there are not standard, interoperable, commercial encryption solutions available. More modern communications methods, which introduce greater security risks, can move toward modern PKI solutions. Older methods still need a technical solution.

Lack of incident reporting

Since utilities are reluctant to share any data on security violations due to the negative publicity that is possible and the potential for this to do damage to stock prices, no clear picture of existing threats based on reliable metrics is available. The North American Electric Reliability Council (NERC) is working on creating a way to do this, but it is unlikely many incidents will be reported due to the negative publicity this brings to the utility. Similarly utilities are reluctant to share this information even with their SCADA vendors. This means that the SCADA vendors' view of the security threats may be understated. If reporting occurred, vendors would also be even more motivated to provide secure solutions due to negative feedback possibilities of their products.

Challenges for SCADA installations

- Single user sign-on procedures to track/audit user activity.

- Security toolkits to secure older products and verify the security with reports.
- Secure operating systems, databases, and applications.
- Interoperable PKI solutions needed for LAN/WAN communications.
 - Interfaces to other systems must be secured.
- Secure device protocols for LAN/WAN communications.
- Secure device protocols for synchronous/asynchronous communications.
 - Low computing power devices still need a technical industry solution that is accepted by NERC and utilities and interoperable between vendors.

Recommendation: Business Process

To be successful, a utility needs corporate security policies in place. Even the best security built in to a SCADA product is insufficient to prevent hacking of a SCADA system if not complemented with a strong security policy and security enforcement program by the users of the SCADA system themselves. This requires:

- A Security Manager
- A Security Awareness Program
- Periodic changes of Username / Password with specials content requirements
 - No More Yellow Sticky Notes!
 - Audits

Internal utility organization models also can impact security solutions. Often, SCADA systems are run within Operations, while the rest of IT is in a separate organization. This is due to the different needs of SCADA systems. SCADA Systems must process

information every two seconds and on demand, so a computer or communication problem cannot be tolerated for any great length of time. IT organizations are not typically suited to respond at the speeds required for SCADA systems. This means dedicated support people are used to support SCADA systems, but this introduces the possibility of disjoint security implementations between operations and IT. Business process within such organizations must be aligned for security solutions.

Recommendation: Research

Support the development of commercial encryption for old low powered devices that are now in operation. The energy industry still needs research for effective and economic encryption for low powered devices, (both wired and wireless), so RTU and other small devices can have encrypted communications. This must then be taken out to become industry standards endorsed by groups such as NERC.

Recommendation: Reporting of both threats and incidents

Promote more widespread reporting of security incidents. Keep this reporting confidential so that a Utility does not fear leaks to the media. Also, a secure way to share threat information with vendors and utilities is needed that does not impact national security. This increases awareness and helps justify investment from the private sector.

Recommendation: Incentives for Utilities to secure their systems

A tax incentive for securing critical infrastructure would be a positive approach to

encourage culture change at electric utilities.

Recommendation: Federal and State cooperation

Electric Utilities can not simply invest in all needed cyber security improvements due to the cost. It is not only a few computer systems that need to be addressed, but their entire control system infrastructure, from the Control Center on out to every monitored substation and on out to each field device (IED). Utilities need to be able to bring these costs into their rate structures, and this can not happen without the support of each state's Public Utilities Commission. Also, non-jurisdictional utilities need to secure their systems as well.

Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action

DHS and DOE have been cooperating, but as with any such large organizations there are still overlaps. This is evident at the National Labs. At Idaho National Laboratory, there is both the National SCADA Testbed (NSTB) (DOE), and the Control System Security and Test Center (CSSC) (DHS). These programs should be combined, and total funding increased for this valuable work. But also, the funding should be committed in advance for a five year period, so that the lab can also test the improvements made in the systems, until systems are judged to be secure. Competition between national labs such as INL, Sandia, PNNL and Oak Ridge for funding and programs should not create confusion in the eyes of the industry as it has in the past. Continued reorganizations and management changes combined with delays in

receiving funding have all contributed to overall delays in security enhancements over the last two years. Interestingly, the people I have met at DHS have been trying to go fast, efficient and cooperative in their work. To me this is a sign of a good culture at work in the organization.

Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds

As a vendor, I represent my customers and their wishes, as well as my company's interests. As a taxpayer, I want to see the security issues resolved as efficiently and effectively as possible, and a risk based approach is the most effective and efficient.

Conclusion

Siemens strongly supports securing the nation's critical infrastructure in many ways. Siemens believes that as a responsible corporate citizen, we have advanced the state of the art in SCADA systems by openly discussing security issues with our customers through our customer association, by creating add-on products for older versions of our products (a Security Toolkit to harden existing installations – a leading innovation in our industry), by participating strongly in standards groups on security of SCADA system (IEC TC57 WG15; NIST PCSRF; DHS PCSF), by having a strong corporate focus on security, and by implementing security programs and standards in our products.

As a SCADA vendor, we have and will continue to develop, implement and advise on

enhanced features and technology to prevent security loopholes. However, in addition to built-in security features for SCADA, it is necessary to merge/complement it with an enterprise wide IT security policy and company cultures that support this. I believe that a form of compliance to security standards is required to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

In conclusion, I appreciate the opportunity to express the views of a leading SCADA manufacturer. We applaud your leadership in examining potential security vulnerabilities to America's vital infrastructure. We believe security compliance is a matter of corporate culture and that this culture must be set and influenced from the very top of every corporation to be effective. By starting at the top of management, I know that the culture of Siemens is one that supports security. We look forward to working with you and the subcommittee in building support for a broader understanding of critical information security issues.

Appendixes to Testimony by

Paul Skare

Product Manager, Marketing

Siemens Power Transmission & Distribution, Inc.

Energy Management & Automation

to the

U.S. Senate Committee on Homeland Security and Governmental Affairs

Subcommittee on Federal Financial Management, Government Information, and International Security

July 19, 2005

Summary or Abstract

- Industry provides the tools to secure SCADA systems even though not all utilities make use of these tools.
- Background on SCADA and SCADA security issues are explained.

Table of Contents:

1	Introduction	3
2	Potential Problems	Error! Bookmark not defined.
2.1	SCADA Vulnerabilities	4
2.1.1	Remote Access	4
2.1.2	Network configurations	4
2.1.3	Disgruntled employees	4
2.1.4	Security holes, patches, viruses	5
2.1.5	Communication protocols not encrypted	5
2.1.6	Lack of incident reporting	5
2.2	Challenges for SCADA installations	5
2.3	Recommendations	6
2.3.1	Recommendation: Business Process	6
2.3.2	Recommendation: Research	6
2.3.3	Recommendation: Reporting of both threats and incidents	6
2.3.4	Recommendation: Incentives for Utilities to secure their systems	7
2.3.5	Recommendation: Federal and State cooperation	7
2.3.6	Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action	7
2.3.7	Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds	7
3	SCADA Vulnerabilities	Error! Bookmark not defined.
3.1	Potential Problems	Error! Bookmark not defined.
3.1.1	Remote Access	Error! Bookmark not defined.
3.1.2	Network configurations	Error! Bookmark not defined.
3.1.3	Disgruntled employees	Error! Bookmark not defined.
3.1.4	Security holes, patches, viruses	Error! Bookmark not defined.
3.1.5	Communication protocols not encrypted	Error! Bookmark not defined.
3.1.6	Lack of incident reporting	Error! Bookmark not defined.
3.2	Challenges to overcome	Error! Bookmark not defined.
3.2.1	Impacts on SCADA Products	Error! Bookmark not defined.
3.2.2	Business Process Impacts	Error! Bookmark not defined.
4	What Siemens has done	7
5	Conclusion	Error! Bookmark not defined.
6	Conclusion	8

Appendix A – What is the SCADA Industry?	8
Appendix B – What is SCADA?	10
Appendix C – What are SCADA Applications?	15
Appendix D – What are SCADA Services?	18
Appendix E – SCADA Security Standards	19
Appendix F – The Use of Biometrics, Smart Cards.....	22
Appendix G – How do you secure SCADA?.....	23
Appendix H – Why aren't SCADA systems already fully secure?.....	25
Appendix I – SCADA Security Education	25

1 Introduction

Good afternoon Chairman Coburn, ranking member Carper, and members of the Subcommittee on Federal Financial Management, Government Information, and International Security. I am Paul Skare, Product Manager at Siemens Power, Transmission and Distribution, Inc. I am representing one of the manufacturers of SCADA (Supervisory Control and Data Acquisition) systems. My role at Siemens includes managing products for SCADA systems as well as substation automation systems. I am also involved in standards groups related to SCADA.

Siemens is one of the largest electronics companies in the world, operating in over 190 countries. We're a diversified company, delivering a wide array of products, systems and services in six main industries. These include information and communications, automation and control, power, healthcare, transportation and lighting. Siemens has over 70,000 employees in the United States across all 50 states.

Siemens' Energy Management and Automation provides software and technologies in regulated and deregulated markets for:

- Single energy suppliers
- Multiple energy suppliers (such as electricity and gas)
- Municipalities
- Generation companies, transmission providers, system operators, and distribution providers in deregulated energy markets
- New participants in the business such as energy traders, balance managers, risk assessors and energy suppliers

- Operators of traction power systems for railways
- Industrial power consumers

A key product for these markets is SCADA. SCADA collects information from devices in the power system, identifies problems, and allows users to remotely control these devices. Adding additional applications to a SCADA allows a more focused and enhanced solution for transmission or distribution systems (referred to as an Energy Management System (EMS) for transmission or a Distribution Management System (DMS) for distribution).

My testimony today focuses on identifying potential security vulnerabilities of SCADA systems, the state of activities related to this, and recommendations to better protect those systems from harmful intrusion.

While our customers primarily use our SCADA systems for the electric system, some also use the same SCADA system for gas, water, and transportation systems. Although our systems are not used as commonly in other settings such as industrial control systems, the concepts are the same across all SCADA systems. In the appendixes of the written testimony, I have provided background information on SCADA and security issues relevant to SCADA. I would like to take this opportunity to congratulate the industry and the government in the work that has been done in the last three years in this area – it has started moving this work from the realm of art to science, and is finally starting to not only spread awareness, but also to get various players to talk the same language.

2 SCADA Vulnerabilities

SCADA vulnerabilities that may be a problem often involve issues associated with the following:

2.1 Remote Access

Remote access to SCADA systems is available for a variety of reasons: user access outside of the control room, user support, and vendor support. This is a problem if there are any accidental (configuration of) security holes. If any backdoors are in the system (either leftover from the vendor or in place for user support), access points are easier to exploit. Local access points must be physically secure or these issues will also apply to them.

2.2 Network configurations

Network (and firewall) configurations are a very important aspect for SCADA systems. SCADA systems depend on a network for operational needs. If a firewall is bypassed accidentally or is miss-configured, a severe security hole could exist.

2.3 Disgruntled employees

If an employee becomes disgruntled, either before or after action by a utility (current or former employees), if the security process has not yet closed all access for that individual, the case for doing damage is greatest, since all the security in place can still be used by an authorized individual.

2.4 Security holes, patches, viruses

Systems rely on standard IT solutions [Commercial Off The Shelf (COTS)] to create a SCADA solution. Some third party security holes in operating systems, commercial databases and other applications can directly translate into security issues for the SCADA.

2.5 Communication protocols not encrypted

Communications, being the largest cost driver in a SCADA solution, is an important area. Since many field devices can last 30 or more years, utilities are reluctant to upgrade them unless there are clear needs. This means many old low power (computationally) devices are in operation, for which there are not standard, interoperable, commercial encryption solutions available. More modern communications methods, which introduce greater security risks, can move toward modern PKI solutions. Older methods still need a technical solution.

2.6 Lack of incident reporting

Since utilities are reluctant to share any data on security violations due to the negative publicity that is possible and the potential for this to do damage to stock prices, no clear picture of existing threats based on reliable metrics is available. The North American Electric Reliability Council (NERC) is working on creating a way to do this, but it is unlikely many incidents will be reported due to the negative publicity this brings to the utility. Similarly utilities are reluctant to share this information even with their SCADA vendors. This means that the SCADA vendors' view of the security threats may be understated. If reporting occurred, vendors would also be even more motivated to provide secure solutions due to negative feedback possibilities of their products.

2.7 Challenges for SCADA installations

- Single user sign-on procedures to track/audit user activity.
- Security toolkits to secure older products and verify the security with reports.
 - To secure operating systems, databases, and applications
- Interoperable PKI solutions needed for LAN/WAN communications.
 - Interfaces to other systems must be secured.
- Secure device protocols for LAN/WAN communications.
 - SCADA login access
 - RTU protocols – DNP over TCP/IP (DNPi)
 - Control Center data links – TASE.2 (ICCP) (Now Available)
 - Interfaces to other systems

Secure device protocols for synchronous/asynchronous communications.

- For synchronous/asynchronous communications - DNP 3.0 & Modbus serial

- Low computing power devices still need a technical industry solution that is accepted by NERC and utilities and interoperable between vendors.

3 Recommendations

3.1 Recommendation: Business Process

To be successful, a utility needs corporate security policies in place. Even the best security built in to a SCADA product is insufficient to prevent hacking of a SCADA system if not complemented with a strong security policy and security enforcement program by the users of the SCADA system themselves. This requires:

- A Security Manager
- A Security Awareness Program
- Periodic changes of Username / Password with specials content requirements
- No More Yellow Sticky Notes!
- Audits

Internal utility organization models also can impact security solutions. Often, SCADA systems are run within Operations, while the rest of IT is in a separate organization. This is due to the different needs of SCADA systems. SCADA Systems must process information every two seconds and on demand, so a computer or communication problem cannot be tolerated for any great length of time. IT organizations are not typically suited to respond at the speeds required for SCADA systems. This means dedicated support people are used to support SCADA systems, but this introduces the possibility of disjoint security implementations between operations and IT. Business process within such organizations must be aligned for security solutions.

3.2 Recommendation: Research

Support the development of commercial encryption for old low powered devices that are now in operation. The energy industry still needs research for effective and economic encryption for low powered devices, (both wired and wireless), so RTU and other small devices can have encrypted communications. This must then be taken out to become industry standards endorsed by groups such as NERC.

3.3 Recommendation: Reporting of both threats and incidents

Promote more widespread reporting of security incidents. Keep this reporting confidential so that a Utility does not fear leaks to the media. Also, a secure way to share threat information with vendors and utilities is needed that does not impact national security. This increases awareness and helps justify investment from the private sector.

3.4 Recommendation: Incentives for Utilities to secure their systems

A tax incentive for securing critical infrastructure would be a positive approach to encourage culture change at electric utilities.

3.5 Recommendation: Federal and State cooperation

Electric Utilities can not simply invest in all needed cyber security improvements due to the cost. It is not only a few computer systems that need to be addressed, but their entire control system infrastructure, from the Control Center on out to every monitored substation and on out to each field device (IED). Utilities need to be able to bring these costs into their rate structures, and this can not happen without the support of each state's Public Utilities Commission. Also, non-jurisdictional utilities need to secure their systems as well.

3.6 Recommendation: Continuing to merge the actions between DHS and DOE into a single cohesive action

DHS and DOE have been cooperating, but as with any such large organizations there are still overlaps. This is evident at the National Labs. At Idaho National Laboratory, there is both the National SCADA Testbed (NSTB) (DOE), and the Control System Security and Test Center (CSSC) (DHS). These programs should be combined, and total funding increased for this valuable work. But also, the funding should be committed in advance for a five year period, so that the lab can also test the improvements made in the systems, until systems are judged to be secure. Competition between national labs such as INL, Sandia, PNNL and Oak Ridge for funding and programs should not create confusion in the eyes of the industry as it has in the past. Continued reorganizations and management changes combined with delays in receiving funding have all contributed to overall delays in security enhancements over the last two years. Interestingly, the people I have met at DHS have been trying to go fast, efficient and cooperative in their work. To me this is a sign of a good culture at work in the organization.

3.7 Recommendation: Embrace Risk based approaches to not only solving the problems, but also in allocating funds

As a vendor, I represent my customers and their wishes, as well as my company's interests. As a taxpayer, I want to see the security issues resolved as efficiently and effectively as possible, and a risk based approach is the most effective and efficient.

4 What Siemens has done

Siemens strongly supports securing the nations critical infrastructure in many ways. We have continued to add more security in our products, we are participating in standards groups to define interoperable security solutions, and we are working with the government and industry groups to promote security.

By starting at the top of management, the culture of Siemens supports security. This is exemplified in the way that Siemens is participating in standards groups and adding security features in our products.

5 Conclusion

Siemens strongly supports securing the nation's critical infrastructure in many ways.

Siemens believes that as a responsible corporate citizen, we have advanced the state of the art in SCADA systems by openly discussing security issues with our customers through our customer association, by creating add-on products for older versions of our products (a Security Toolkit to harden existing installations – a leading innovation in our industry), by participating strongly in standards groups on security of SCADA system (IEC TC57 WG15; NIST PCSRF; DHS PCSF), by having a strong corporate focus on security, and by implementing security programs and standards in our products.

As a SCADA vendor, we have and will continue to develop, implement and advise on enhanced features and technology to prevent security loopholes. However, in addition to built-in security features for SCADA, it is necessary to merge/complement it with an enterprise wide IT security policy and company cultures that support this. I believe that a form of compliance to security standards is required to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

The energy industry still needs research for effective and economic encryption for low powered devices, (like RTUs and even transmitters), so RTU and other small devices can have encrypted communications.

However, as a SCADA vendor, it is not possible to force our customers to buy all security offerings, nor to use the built-in security aspects of our products. Even the best security built-into a SCADA product is insufficient to prevent hacking of a SCADA system if it is not complemented with a strong security policy and security enforcement program by the users of the SCADA systems themselves.

Siemens input on the subject is that security compliance is a matter of corporate culture, and that this culture must be set and influenced from the very top of every corporation to be effective.

Siemens believes that a form of regulation/compliance to security standards is the only way to ensure that utilities will adopt sufficient security measures to truly safeguard the electric infrastructure of the United States. These standards will be most successful when created through open partnerships of government and industry.

In conclusion, I appreciate the opportunity to express the views of a leading SCADA manufacturer. We applaud your leadership in examining potential security vulnerabilities to America's vital infrastructure. We believe security compliance is a matter of corporate culture and that this culture must be set and influenced from the very top of every corporation to be effective. By starting at the top of management, I know that the culture of Siemens is one that supports security. We look forward to working with you and the subcommittee in building support for a broader understanding of critical information security issues.

Appendix A – What is the SCADA Industry?

Market

The SCADA and Energy Management System industry for high voltage electric transmission is a global market served by a very small number of large engineering firms and one dominant consulting organization. The important market forces that have shaped this industry include:

- A relatively small, and decreasing number of potential customers worldwide
- Very complex system requirements
- High R&D cost of market entry
- Low industry investment (perceived value) in systems upgrade / replacement
- High risks to technical and commercial success in systems delivery

Especially in recent years as investments in the transmission infrastructure in the U.S. have declined, there have been very few new system orders and technology previously delivered has in some cases not been well

maintained. Due to long project definition / delivery cycles and limited investments in maintenance and upgrades, the in-service SCADA infrastructure has significantly lagged the general information technology infrastructure.

Current business drivers within electric utilities are forcing integration of legacy (and in some cases obsolete) SCADA technology to other business systems and non-operational users at a rapid pace. This situation is creating new challenges for maintaining security on these proprietary systems originally designed to operate in isolation.

For Utilities to successfully cost justify the additional investments associated with security initiatives, a solid business case must be presented. Preparation of such a business case should include a security risk assessment including:

- Proving that threats are real and happening
- Using a common tool against your network and report on the attempt
- Assessing the impact an attack could have on your utility's reputation/profits
- Assessing the impact that a Denial of Service attack could have on your utility's reputation/profits
- Providing metrics to management on Internet attacks, companies affected, and damage caused
- Considering insider risks including all aspects of Internet usage
- Retaining a third party to perform a vulnerability assessment

Industry

While there are many niche vendors and small vendors of software in this business space, there are four major SCADA vendors: Siemens, Areva, ABB and GE (GE has been less and less engaged at the high end of the market). Some large SCADA systems require large bonds to be posted in order to bid on a order, and require a history of having delivered large systems due to the high importance of SCADA systems to everyone's infrastructure. All the big vendors have extensive presence internationally in this business, with business activities also spread out internationally. In the case of Siemens, development, delivery and support of the SCADA software is performed in Minneapolis (Minnetonka), Minnesota, USA as well as in Nuremberg, Germany.

When a utility determines it needs a new SCADA system, they will either write a specification (Request for Proposal – RFP) for the new SCADA system internally, or contract with a consultant to write one for them. These RFPs, along with the industry and IT standards, and NERC policies/standards greatly influence what vendors develop for their base products.

Vendors who are invited to bid on the order review the RFP, determine the aspects of the RFP that they can comply with, and propose a price based on the aspects of the RFP that they agree to meet.

The utility, typically together with the consultant, then evaluate the bids, and determine who has the best price for the needed requirements. An internally weighting is typically applied to the bids with unknown scales from the vendor's perspective.

Once a vendor is chosen, and a contract is signed, the project begins.

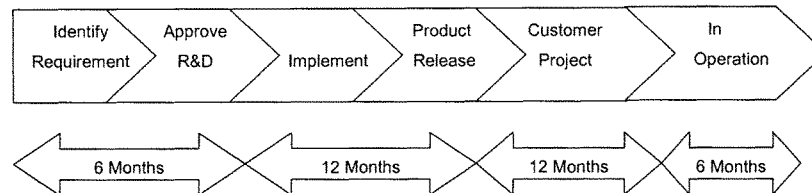
Dependence on mainstream IT

Due to the economic situation and the standards based requirements in the industry, we are dependant on the mainstream Information Technology (IT) world for security technology specifically, and for IT technology in general.

Product Delivery Influences

Delivery Timescales – Idea to R&D to project to field

Typical product delivery cycles include:

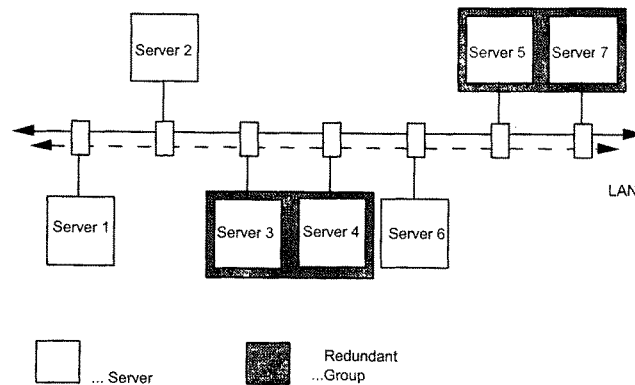


It is typical for some of these cycles to overlap, and all these numbers are samples that are typical, but vary widely. The sales cycle on these projects are commonly measured in years for new medium to large projects, in quarters for add-on, upgrade, and small projects.

The business cycle from the utility perspective can also be much longer, including rate cases with state PUCs, evaluating requirements, writing specifications, etc. Commercial projects have significant lag times between bookings and sales – from 3 to 48 months depending on the size of the project. The high end of the market is most prone to these effects, since there are few projects nationally each year, and each one has a higher degree of customization compared to lower level projects (at lower voltage levels) which rely more on base product approaches with lower levels of customization.

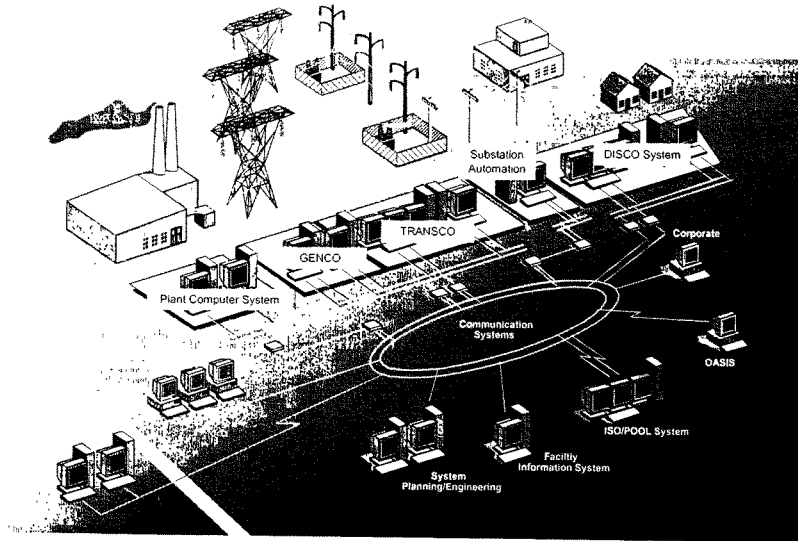
Appendix B – What is SCADA?

Supervisory Control And Data Acquisition (SCADA) systems collect data from substations, power plants, and other control centers. They then process the data, and allow for control actions to be sent back out. Other names of systems that can include SCADA include Energy Management Systems (EMS) and Distribution Management Systems (DMS). Typically these systems provide additional features on top of the basic SCADA, targeting either the transmission or distribution grids. SCADA systems are typically distributed on several servers connected via a redundant Local Area Network (LAN). A Utility's enterprise SCADA system might consist of anywhere from 2 to 150 computers. The SCADA itself does not include Remote Terminal Units (RTUs), devices, or computer networks and firewalls.

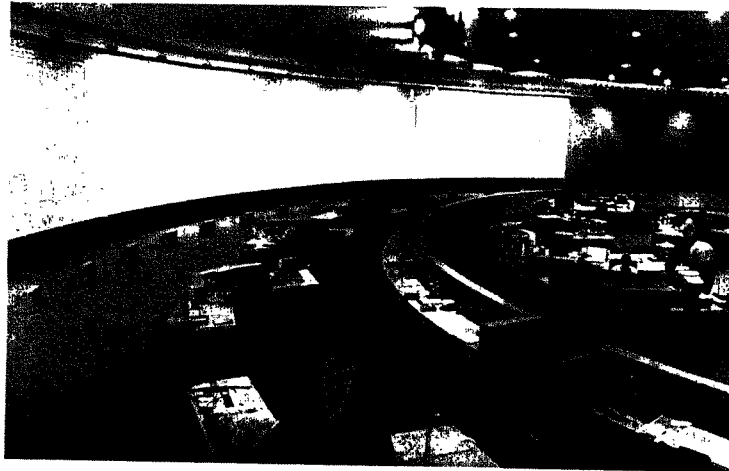


911B

SCADA systems are typically run by an operations group in a central location for an electric utility. The following picture shows the systems a SCADA system usually communicates with. Deregulation has contributed to the entities who must communicate.

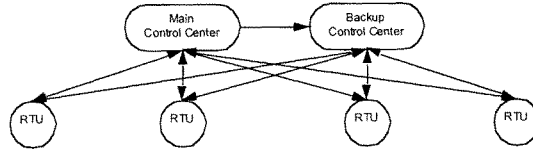


Below is a picture that shows how a SCADA control center appears much like NASA's Mission Control Center.

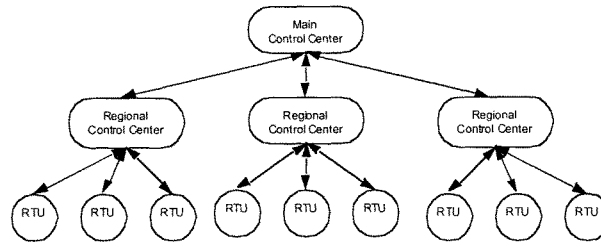


SCADA systems often have emergency back-up configurations.

A Typical Configuration (geographically separate backup location)



A Regional configuration



They communicate externally in a variety of ways. They use leased phone lines, dial-up phone lines, and LAN/WAN communications. These are usually provided by a local telecom. In addition, devices are commonly connected to the remote ends by additional communication methods, including hard wire contacts, radio, satellite, and microwave. Wireless technologies are being used more and more for connections to sensors.

These different methods of communication are used due to both economic and geographic reasons. All telemetry is expensive, but the more there is provides for a better understanding of the conditions of the electrical grid. Some places are quite remote and local telecom providers do not cover all areas needed. Further, some types of telemetry are of lower priority than others, so they can use less expensive, capable, or reliable means to get the data.

All decisions on communications methods are a business decision each Electric Utility makes. This includes not only the quantity and method of communication, but also the security involved with this communication.

Devices that SCADA systems communicate with typically are Remote Terminal Units (RTUs) that are in a substation or power plant, and hardwired to other devices to bring back meaningful information, such as current MW, MVAR, AMPS, volts, etc. More and more, Intelligent Electronic Devices (IEDs) are being used that can be connected directly to the SCADA systems or indirectly by means of a gateway computer (RTU).

The protocols that are used to communicate with RTUs have evolved over time as technology has progressed. Early protocols are Synchronous in nature (bit oriented – with a separate timing signal). They are very efficient, but do not have a lot of features, and require special hardware to operate. As PCs hit the market, Asynchronous (byte oriented – using standard serial ports) protocols became more popular. They used more computing power

and bandwidth, but supported faster speeds and more complex commands. Recently, TCP/IP based protocols have been growing in popularity, due to yet more complex command possibilities, and the proliferation of LAN/WAN communications and smarter devices. Telecoms have been spurring this on by raising prices on leased lines (used by synchronous/asynchronous communications), and lowering costs for frame relay connections (used by TCP/IP based communications). Technology has been spurring this on by providing more features and higher speeds by using TCP/IP based connections rather than serial communications.

Network connections in a SCADA system are connected via hubs, switches, routers and firewalls. A SCADA system is normally firewalled inside a utility's corporate firewalls, providing for a double level of firewall protection. Communication connections to the telecom for RTU communications typically bypass these firewalls. In the US, SCADA Vendors do not normally provide the network infrastructure or firewalls, but instead rely in the utility for these things, since most utilities have IT/MIS departments that provide these.

Interfaces to other systems

A SCADA system is increasingly connected to more and more systems in a Utility. Examples include:

- Asset Management (AM) / Facilities Management (FM) / Geographic Information System (GIS)
- Corporate Computer / Billing / CIS
- Trouble Call
- Load Management
- Corporate Dashboards

Each system that is connected to a SCADA system then becomes a security issue to make sure that all sides have adequate security in place. Most interfaces like those listed above are with other vendors' products. Enterprise Application Integration is an emerging trend used to connect these systems.

Control Center to Internet

Due to the proliferation of Internet based applications, such as e-tagging and OASIS, as well as e-mail and web site access, the Internet is connected more and more often to SCADA systems. This does not mean that a User Interface to the SCADA system is made available to the public Internet as is depicted in techno-thrillers made for TV, rather that there are multiple tiers of firewalls between the two. The risk is primarily of accidental connection or improperly configured firewalls and routers by the owners of the systems.

Control Center & Wireless

Some utilities have used wireless technologies, typically for remote crews working in the field and for monitoring of alarms in the SCADA system. Other uses include radio/satellite/wireless communication technologies to access remote locations where wired communication is either not possible or is economically disadvantageous. Any wireless communication can be a security threat if not encrypted, but encryption on small devices is often beyond the capabilities of small inexpensive field devices due to the computational requirements to encrypt communications. Wireless communications includes IEEE 802.11, Mobile phones (GSM/GPRS/SMS), and Bluetooth.

Telecom Dependencies

For most Electric Utilities, they are dependant on the local telecom provider for most communications between the control center and the external world. In particular, the control center to substation communication that typically either uses leased or dial-up phone lines and frame relay networks. Any security issue at the telecom provider becomes a security issue for the utility's SCADA system.

Third Party Security Solutions

SCADA vendors and their dependence on third party products create a security issue in their use of those third party products. Computer Hardware, Operating Systems, and Relational Databases are examples where SCADA vendors are dependant on third parties for major aspects of a SCADA solution. If the IT world and these

third party vendors have security issues, then the SCADA systems will have those same security issues. Some third party products offer an overview of security related issues.

Example: IBM Tivoli Netview

- Standardized security management over multiple platforms (AIX, NT, MVS)
- Produces audit trail
- Reports all events to a centralized source
- TACF (Tivoli Access Control Facility)
- Monitor/control access to selected system resources on a per-user basis
- Used to secure root and other common IDs.
- Logfile adapter monitors /var/adm/messages
- Plus modules for
 - ADSM backups
 - Oracle

Appendix C – What are SCADA Applications?

This section defines the security related functions within a SCADA system.

SCADA

Load Shed: manual and rotating: to drop load safely during emergencies – manually to select specific areas, rotating to spread the loss around.

Under Frequency Load Shed: To drop load safely based on under frequency conditions.

Alarm Processing: Notify users of problems in the system.

EMS Applications

Transmission Network Security

- Model Update: Update the data model of the network based on real-time inputs.
- State Estimator: Estimate values of non-telemetered points.
- Optimal Power Flow: Calculate power flows on transmission lines.
- Security Analysis: Study/Perform what-if scenarios based on loss of equipment in the grid.
- Voltage Stability Analysis: Study conditions in real-time that could lead to a voltage collapse.
- Dynamic Stability Analysis: Study conditions in real-time that could lead to dynamic instabilities.
- Operator Training Simulator: For training of users in normal operations, emergency operations, and system restoration activities.

Decision Support Tools in Systems Operation

Considering the events that led up to the recent and historic blackout of August 14, 2003, as well as the ramifications to the transmission system and the general population, it is clear that attention is being drawn to the reliability of the transmission system throughout the country. Although this particular event is not yet fully understood, it is true that many analysis tools exist today but are currently being underutilized as investments in the transmission infrastructure have stagnated. There are few systems indeed that fully utilize existing

capabilities in understanding the current real-time state of the network, its vulnerabilities to foreseeable events, its alternate and safer modes of operation, and its behavior during significantly degraded operations.

As the safety margins originally designed into the transmission system have all but disappeared through increasing loads, lagging investments, and new economic forces, it has become imperative that operations personnel have the clearest possible view of their transmission networks, be well trained for emergency operations, and be armed with effective decision support tools. The good news is that this technology not only exists today, but it can also be deployed in short order. Grid operators and utilities can take immediate advantage of System Analysis, Decision Support and Training tools from Siemens that can be quickly interfaced to an existing SCADA / EMS installations using industry standard technologies. There is no need to think in terms of wholesale system replacement in order to modernize your EMS.

What follows is a simple summary of the role and importance of existing network analysis tools, tools each of which have been deployed many times and on many different architectures throughout the energy industry. Through its Energy Management and Information Systems Division, Siemens has worldwide experience and expertise in getting these tools into production quickly and reliably. We believe that your goal of 100% reliability in the transmission system can only be achieved through proactive use of proven decision support tools, emergency procedure development, and comprehensive operator training. Siemens also has the integration tools, and the experience to incorporate these tools into your operation successfully.

State Estimation – As an adjunct to SCADA data processing, the State Estimator provides a simple and cohesive view of the real-time state of the entire transmission system, including a look into the health of neighboring networks as well as clearly representing the existence of "electrical islands". The State Estimator also identifies, and compensates for failures in the SCADA software subsystem, data telemetry, and local metering so that issues obscuring a proper view of the transmission system may be corrected proactively, not discovered during system emergencies or post-mortem analyses. New innovations in State Estimation now include the direct use of GPS provided Phase Angle measurements enabling more complete, and more robust solutions.

Intelligent Alarm Processing – In today's large systems high volumes of alarms are a fact of life. Coupled with old technology or poor user presentation, sometimes the most important system events are too easily overlooked or root causes impossible to determine. An intelligent alarm processor add-on not only ensures the operator sees the most important information, but also determines the root causes for cascading alarm situations immediately, and summarizes system problems involving hundreds of alarms simply. In times of seeming quiescence, the Intelligent Alarm Processor ensures that issues of low priority but significant duration, such as slow frequency oscillations, are not overlooked.

Security Analysis / Optimal Power Flow – You need to be aware, in advance, which potential system events will result in a degraded system operation that is simply unacceptable. Armed with real-time operational knowledge, the transmission system can be steered to a state which is not only secure during normal operations, but that will also remain secure in the event that any contingency becomes reality.

Dynamic Stability Analysis / Voltage Stability Analysis – These problems, usually well studied in the planning environment, are the most difficult to predict intuitively in the real-time operations environment. Although high loads and transmission stress can be an indicator of a potential problem, so can many other factors such as minimal loading, generation mix, load distribution, etc. Considering that the transmission grid is now often operated in an economic environment not planned for or well studied, on-line Dynamic Stability and Voltage Stability Analysis ensure that operators are alerted to conditions that could potentially lead to dynamic instabilities and voltage collapse.

Restoration Assistance – Should the worst happen and your system suffer a partial or complete shutdown, your Restoration Assistant becomes an invaluable tool for saving time and equipment during the extraordinarily complex task of system restoration. The Siemens Restoration Assistant can plan out an overall restoration strategy in minutes, or simply perform advance checks on switching operations such that generation, load, voltage and VAR supply all remain within critical balances. The Assistant also ensures that operations personnel understand the possible consequences of reconnecting your operational system with a neighboring system in order to support their restoration activities.

Simulation and Training – There can be no substitute for well-trained operational personnel. Their actions during critical situations equate directly to either the continued healthy operation of the system, or its being set on a course toward failure. Just like airline pilots that rely on well-planned emergency procedures and have trained exhaustively for failures in the sky, your operations staff needs to have developed and tested their emergency plans as well. Each and every operator needs the opportunity for emergency simulation training in order to safely carry their system through foreseeable emergency conditions. The Siemens Training Simulator is based on the open EPRI architecture model, resulting in a tool which can be plugged into your existing SCADA / EMS to provide simulation and training capabilities in an environment your operations personnel are already accustomed to.

Improved Data Modeling – Many transmission networks are modeled using outdated processes and tools, leading inherently to analysis errors in the operations environment. The Siemens Information Model manager (IMM), employs the latest in web-based deployment and visualization. All data is modeled within the industry standard Common Information Model (CIM), and is represented both within that structure as well as graphically – leading to efficient and accurate model checkout, and automatic one-line diagram generation. The standard formats used for data model and graphics exchange make interfacing this productivity tool to your system both simple and straightforward.

Historical Data Storage and Recovery – Having the ability to quickly, accurately, and efficiently store and recover historical data from your transmission system is critical to analyzing problems and developing effective operational solutions. Tools like the Siemens Historical Information System (HIS) are essential in today's environment. Accurate recording, archiving and quick recovery of essential operational data is necessary to ensure you operate your system within reliability standards, and to develop and test remedial action plans for those circumstances where reliability may have been compromised.

Operating your transmission system has always been a complex task. Thankfully, catastrophic failures have been rare, but also not rare enough. There is no question that the risks and consequences of failures are increasing. However, there are tools available today that can help to mitigate the challenges facing your system's grid operators. These tools and more are continually being developed and perfected by Siemens to help ensure the reliability, stability and security of one of the most important pieces of infrastructure in the world – the North American transmission grid.

DMS Applications

Distribution Network Applications

- Distribution System Power Flow: Determine power flows in the radial distribution network.
- Fault Location: Locate fault locations.
- Fault Isolation and Service Restoration: reroute distribution network to isolate faults and restore service.
- Volt/Var Control: Adjust volts/vars to more economically distribute power.

- Optimal Feeder Reconfiguration: Reconfigure the feeders based on system conditions.

Outage Analysis

- Outage Management System: Report and coordinate outages.
- Switching Procedure Management: Allow for collections of multiple control actions.

Energy Scheduling Applications**OASIS**

This Internet based system allows market entities to buy transmission capacity on the grid.

E-Tagging

This Internet based system allows market entities to schedule the actual energy on the grid, previously arranged via OASIS.

RTUs/IEDs/other devices

These are the end devices that the SCADA system communicates with. Typically they are low non-powerful computing devices of various sorts, and do not have the computing strength for encryption. While newer devices are being developed with the necessary strength, older lower speed devices will continue to be in operation for decades to come. RTUs can have a lifetime of up to 50 years. Various studies estimate it costs a utility approximately \$100,000 to put a new RTU in a substation. These costs are from the cost of the new RTU itself, the connection and installation of the new RTU, the configuration and tuning of the measurements of the RTU, the data maintenance needed in the SCADA system to properly define the new RTU and modify the SCADA displays that refer to the RTU. Repeated trips by field crews to the substation in coordination of personnel on the SCADA system are typically needed.

Substation Automation

As automation technology progresses to more quickly deal with protection, control, and metering issues in the substation, computers providing the solution also become security issues.

Appendix D – What are SCADA Services?**Maintenance Agreements**

These are agreements between the SCADA vendor and the electric utility to provide experts to work on the SCADA system at predefined rates based on the amount of hours per year needed.

Software Subscription service

These are agreements between the SCADA vendor and the electric utility to provide new version of the base software when they are released based on a percentage of the intellectual property rights paid on a periodic basis.

Patch Management/Security service

A Subscription Based Security Information Service for Siemens SCADA

- Receive applicable Software Security Alerts for SPECTRUM and Third-Party Software – from Siemens
- Receive SPECTRUM Security Toolkit Upgrades – Harden your SPECTRUM System

Expected Future Additions

- Additional SCADA Products
- Industry Analysis
- Security Training Programs

SIEMENS

Report

Third Party Product Emergency Updates are used in the analysis

- Rollup of Third Party Product Updates
- CERT- Computer Emergency Response Team
 - SEI CERT- Software Engineering Institute
 - Siemens CERT- Siemens Corporate CERT
- ISAC- Information Sharing and Analysis Center Electricity Sector
- NIPC- National Infrastructure Protection Center

Optional Security Services

- Auditing Setup
- Run Penetration tests
- Implement Security Policy (e.g., SAS-70)
- Review Security Policy
- Incident Handling Procedures
- Certificate Authority

Application Service Providers (ASPs)

These applications are emerging as an economic alternative to ownership for utilities. They can access these applications over secure networks, and either pay on demand or pay monthly fees for access to the applications.

- Major offerings to date
 - Certificate Authority / Management
 - OASIS
 - E-Tag
 - Market Systems
- Requirements
 - Physically Secure Facility
 - Redundant Power Supply (computers, UPS, generation)
 - Redundant and Secure Communication Infrastructure

Appendix E – SCADA Security Standards

Existing Standards

While numerous standards bodies exist in the industry, the overall top level standards specific to electric utilities use of SCADA systems is the International Electrotechnical Commission (IEC) Technical Committee 57 - Power System Control and Associated Communications. In the US, the IEC operates in association with the American National Standards Institute (ANSI).

The IEC is one of the bodies recognized by the World Trade Organization (WTO) and entrusted by it to monitor the national and regional organizations agreeing to use the IEC's International Standards as the basis for national or regional standards as part of the WTO's Technical Barriers to Trade Agreement. [see <http://www.iec.ch/about/partners/agreements/wto-e.htm> for details].

The IEC works closely with its international standardization partners, the International Organization for Standardization (ISO) and the International Telecommunication Union (ITU), other regional standardization

SIEMENS

Report

organizations and international organizations, including the International Commission on Illumination (CIE), the International Council on Large Electric Systems (CIGRE), and the Union of the Electricity Industry (EURELECTRIC).

Security specific groups include:

Other groups with influence include the IEEE, IEE, NERC, FERC, NAESB, NRECA, EPRI, OMG, OAG, OPC Foundation, DOE, DHS, CIGRE, ITU-T, NIST, UCTE (former UCPTC), DNP User's Group, UCA International User's Group, the Whitehouse, National Labs.

EPRI: Enterprise Infrastructure Security (EIS)

IEC TC 57: WG 15

CERT- Computer Emergency Response Team (Carnegie Mellon University)

SEI CERT- Software Engineering Institute

Siemens CERT- Siemens Corporate CERT

ISAC- Information Sharing and Analysis Center (Electricity Sector)

NIPC- National Infrastructure Protection Center

Working Groups

Following is a list of active working groups within the IEC TC57:

WG 3: Telecontrol protocols

WG 7: Telecontrol protocols compatible with ISO standards and ITU-T recommendations

WG 9: Distribution automation using distribution line carrier systems

WG 10, 11, 12: Communication standards for substations:

WG 10: Functional architecture and general requirements

WG 11: Communications within and between unit and station levels

WG 12: Communication within and between process and unit level

WG 13: Energy management system application program interface (EMS - API)

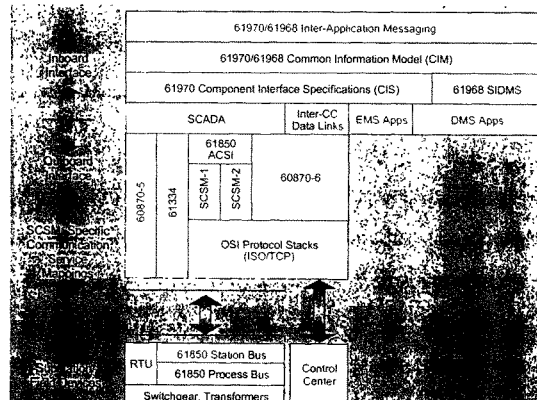
WG 14: System interfaces for distribution management (SIDM)

WG 15: Data and communication security

WG 16: Framework for deregulated electricity market communications

WG 19: Interoperability within TC 57 in the long term – responsible for the Reference Architecture

Graphical Overview of standards for SCADA



IEC TC57 WG15: Data and Communications Security

Mandate: Provide direction and assist other Working Groups Secure their protocols

Members of working group 15 come from consultants, vendors, utilities, and US national labs.

WG15 – Protocols and Groups Affected

	Number	Scope	Protocols	TC57 WGs
RTUs	IEC 60870-5	Telecontrol	101, 102, 103, 104, DNP	3
Data Links	IEC 60870-6	Control Center	104, DNP	7
Meters	IEC 61334	Meter Reading	DLMS	9 and TC13
	IEC 61850	Control Centers, Substations	MMS, 60870-5	10,11,12
All of the above	IEC 61970, IEC 61968	CC Application Interfaces	None yet	13,14
APIs				

Non-IEC as well!

WG 15 Recommendations

- Use consequence-based analysis
- Provide multiple levels of security
- Focus on application layer
- Work together with other IEC TC 57 Working Groups
- Address key management
- Address the complete system
- Use ISO 15408 process (streamlined)

THREATS	DUTIES	GOALS
Denial of Service	Be thorough	Confidentiality
Replay	Be clear and concise	Authentication of Data
Access to strong points via weak points	Consult all stakeholders	Authentication of Source
Traffic Analysis	Make it interoperable	Integrity of Data
Impersonation	Make it safe and secure!	
Hijacking connections		
Disgruntled insiders		

Related Security Standards

IEEE Standard 1402-2000

IEEE Guide for Electric Power Substation Physical and Electronic Security

Provides definitions, parameters that influence threat of intrusions, and gives a criteria for substation security

Cyber methods considered:

- Passwords
- Dial-back verification
- Selective access
- Virus scans
- Encryption and encoding

NERC Security Policies

NERC Security Guidelines for the Electricity Sector: <http://www.esisac.com/publicdocs/Guides>

NERC Cyber Security Standards:

<http://www.nerc.com/~filez/standards-cyber.html>

SAS – 70 Security Standard

SAS-70 Audit

- Statement on Auditing Standards No. 70
- Audit procedure for Service Organizations that handle data and financial transactions
- Reports on the processing of Transactions by Service Organizations
- Audits company's ability to maintain systems so the data is secure and reports are secure and financially correct
- Many Companies accept SAS-70 results so they don't have to audit external companies individually.

Scope of SAS-70

- Documentation
- Data security
- Privacy of information
- Prevention of theft
- Availability of systems
- Authentication of sender and receiver
- Data integrity
- Controls
- Change Management Process
- Authorized access
- System backup and recovery procedures

Appendix F – The Use of Biometrics, Smart Cards

Advancing automation and the development of new technological systems, such as the internet and cellular phones, have led users to more frequent use of technical means rather than human beings in receiving

authorization. Personal identification has taken the form of secret passwords and PINs. Everyday examples requiring a password include the ATM, the cellular phone, or internet access on a personal computer. In order that a password cannot be guessed, it should be as long as possible, not appear in a dictionary, and include symbols such as +, -, %, or #. Moreover, for security purposes, a password should never be written down, never be given to another person, and should be changed at least every three months. When one considers that many people today need up to 30 passwords, most of which are rarely used, and that the expense and annoyance of a forgotten password is enormous, it is clear that users are forced to sacrifice security due to memory limitations. While the password is very machine friendly, it is far from user-friendly.

There is a solution that returns to the ways of nature. In order to identify an individual, humans differentiate between physical features such as facial structure or sound of the voice. Biometrics, as the science of measuring and compiling distinguishing physical features, now recognizes many further features as ideal for the definite identification of even an identical twin. Examples include a fingerprint, the iris, and vein structure. In order to perform recognition tasks at the level of the human brain (assuming that the brain would only use one single biometric trait), 100 million computations per second are required. Only recently have standard PCs reached this speed, and at the same time, the sensors required to measure traits are becoming cheaper and cheaper. Therefore, the time has come to replace the password with a more user-friendly solution -- biometric authorization.

Appendix G – How do you secure SCADA?

Actions Needed to Secure SCADA

- Secure Applications and Relational Database Access
 - Username/Password, roles, services, administrative authorities all must be set
- Operating System
 - Disable unused services and ports
 - Directory and file permission settings
 - Username/Password administration and auditing
 - User logon to domain
 - Authorization (restrict access to resources you have been assigned)
 - Resources assigned to individual or groups
 - Access Control Lists
 - Authentication (verify who you are)
 - Biometrics Options
 - Siemens ID Mouse with a capacitive sensor for fingerprint biometrics for logon.
 - Smart cards are an alternative to biometrics that relies on a possession for authentication.
- Network Communications
 - Deploy appropriate routers, firewalls, intrusion detection systems, Identify Security Administrator to manage security. Includes intrusion detection, intrusion prevention systems.

Physical Security

Guards and associated physical security are not part of a vendor's SCADA solution. They are specific to each Electric Utility.

Physical Security Monitoring

Monitoring of Physical Security issues can be done through the use of a SCADA system. Contacts can be wired for door access in substations as well as control rooms, and fed back into the SCADA system as a digital value. An Alarm category can be set up specifically for physical security violations, and this alarm category would be logged. A SCADA Display can be created to graphically display any security violations on a system basis. This type of capability is available via off the shelf software in most SCADA systems. This would typically be used as an operational back up of primary security systems.

Functional Security

Functional security is the area where SCADA applications must implement specific security technologies in order for the function to work. For example the Inter Control-Center Communication Protocol (ICCP) known as TASE.2 in the IEC has recently added a PKI solution to the international standard of ICCP. This required changes to the ICCP function itself in order to be possible.

Example: Siemens SCADA Security Toolkit

In order to provide for a secure Siemens SCADA solution on current and older version of the SCADA product, we have created a Security Toolkit. This evolving toolkit consists of a collection of utilities that allow the SCADA owner to tighten and monitor the security of the SCADA system. These utilities can be run once, or periodically automatically, and consider:

- Access policy (Host/LAN/VPN)
- Router/firewall configuration
- OS root/user username access
- UNIX services/programs
- Remote command usage
- FTP Usage by Applications
- Directory/file access rights
- RDBMS security
- Application passwords/authorities
- Integrity Scan (verify that SCADA program binaries have not been altered without authorization)

Other Solutions

The use of a Public/Private Key Infrastructure (PKI) solution addresses the following issues:

- **Privacy:** No one other than the parties or systems involved knows the details of the electronic messages. This is accomplished through the use of Encryption using Cryptographic Protocols;
- **Authentication:** All parties to a transaction or electronic message exchange know whom they are dealing with at the outset. This provides proof of identity through the use of UN/PW logins with Digital Certificates, Smart Cards, Biometrics.
- **Integrity:** Messages cannot be changed while in transit between parties or systems; and
- **Non-Repudiation:** A party cannot deny having engaged in a transaction or having sent an electronic message.

The following issues must be met via other solutions:

- **Protection (of Resources):** Firewall, DoS Protection, Content Filtering, Virus Scanning, and Intrusion Detection are all areas that traditional IT solutions usually are applied.
- **Authorization:** A party is set up to provide the Certificate Authority and User Name and Password administration, as well as any setup of biometrics. This can be an internal or external group but is dependant on the policies and organizational structure at a utility.
- **Physical Security:** The normal 'guards and guns' type security, along with monitoring and surveillance capabilities is either in house or contracted out depending on the utility. Badge or smart card accesses to SCADA areas within buildings are normally coordinated through here.

Appendix H – Why aren't SCADA systems already fully secure?

SCADA systems have only recently (in the last 10 years) been connected to other IT technologies in a significant fashion. Previously SCADA systems were very isolated. Now that SCADA systems are increasingly connected to the outside IT world, and Cyber security solutions have begun to find mainstream adoption, it is time to make sure SCADA systems are secure. There are numerous negative side effects that have been mentioned in the past that have slowed implementation of a strong security environment for SCADA users.

- One is that it is more difficult to use the system. Every user must individually login and logoff when using the system.
- Maintenance support is more time consuming due to the restrictions of putting quick fixes into the system must now go through more rigorous security measures to verify the legitimacy of the fix.
- A security policy is only good if it has a manager and periodic audits: This adds a lot of cost to the environment, as well as inconvenience by having periodic audits.
- Periodically being forced to change passwords is tedious and irritating, but it is something that users can grow accustomed to.
- Acquiring and changing Digital Certificates as needed is an additional cost and time consuming affair. Since Digital Certificates have limited life spans, this is an ongoing, recurring effort and expense.
- All security features of a SCADA system cost the vendor R&D and maintenance costs.

While none of the above effects should be showstoppers, they are frequently referred to and complained about. A successful security initiative must address these issues from the point of view of showing the overall benefits to the company.

Appendix I – SCADA Security Education

Siemens SCADA Customers

Siemens customers have a customer association that meets twice a year. It is named SECA (Siemens EMIS Customer Association). This meeting has a session/presentation about security at each meeting. Discussions about security features in the Siemens products, and feedback on security issues to Siemens are all features of these meetings. Panel sessions discussing real-world issues faced by SCADA users allow members to exchange information between each other as well as with Siemens. Bringing in industry experts (such as Jeff Dagle, Pacific Northwest National Laboratory in Richland, Washington) to discuss SCADA Security issues to the membership are also an example of the types of security discussions held at SECA meetings.

NERC Security Workshops

SIEMENS

Report

NERC is holding security workshops to heighten awareness of security issues for Electric Utilities. Other consulting groups are also holding security workshops, however there is a feeling that some are trying to take advantage of the situation.

NERC Security Status

NERC is also providing the industry with the current status of security threats at the national level. Below is an example of this.

Electricity Sector Threat Advisory Levels	
Physical ELEVATED ■ ■ ■ Significant Risk of Terrorist Attacks	Cyber ELEVATED ■ ■ ■ Significant Risk of Terrorist Attacks

Security Policy

An example of a good starting point for a security policy is through the use of the SAS-70 standard. This standard is already in use by some of the larger Utilities. The new NERC security guidelines are also a good description of what is needed for the control room.

More Security Information

See SANS (<http://www.sans.org>) for generic IT security information and information like this:

1. Key Elements of successful security awareness Program:
 - provide training on regular basis and include as part of new employee orientation program
 - Keep users informed about current trends in computer incidents
 - View security awareness as an on-going requirement
2. Key Elements of good security infrastructure:
 - Establish roadmap for security infrastructure improvements
 - Strong commitment from senior management to support security improvement roadmap
 - Metrics to measure security vulnerabilities and report to senior management
 - Understand risks to your environment
 - Justify the security infrastructure environment (potential impact to company's reputation/revenue)
3. Common Security Problems:
 - Administrators not properly trained in the area of information/network security
 - Administrators do not have upper management support to deploy appropriate security measures
 - Sites do not install security patches in a timely manner
 - Sites do not filter incoming mail for possible hostile attacks
 - Sites do update anti-virus software signature files on regular basis (should be automated procedure)
4. Common management errors:
 - Focus on reactive, short-term fixes resulting in problems re-emerging at later date
 - Rely only on a firewall for security perimeter protection

SIEMENS

Report

Fail to realize the value of their information and data

Fail to understand relationship of information security to the business (understand physical security but not consequence of poor information security)

SANS has a list of recommended steps to follow when responding to an incident. They are:

- Follow your policies and procedures
- Contact appropriate agencies
- Use 'out-of band' communications (like phone calls) to avoid intruders being notified of response
- Document your actions with good notes in chronological order
- Make a complete system backup and keep safe with a positive chain of custody
- If you are unsure of what actions to take, seek help before removing files or halting system processes
- Contact local law enforcement (police or FBI) for advice and assistance as soon as possible

The new NERC policies also cover this via the Electricity Sector Information Sharing and Analysis Center (ES-ISAC) at <http://www.esisac.com>

<http://www.incidents.org> (by SANS institute)

<http://icat.nist.gov> (NIST security computer division)

<http://cve.mitre.org> (Common Vulnerabilities and Exposure)

<http://xforce.iss.net> (Internet Security Systems)

<http://seclab.cs.ucdavis.edu/projects/vulnerabilities/#database/> (Univ of Calif Vulnerabilities Project)

<http://www.cs.purdue.edu/coast/projects/vdb.htm> (Univ of Purdue Cooperative Vulnerabilities Database)

<http://www.siemens.com/biometrics> (Siemens Biometrics)



TESTIMONY OF
THE HONORABLE THOMAS JARRETT
SECRETARY AND CIO, DELAWARE DEPARTMENT OF
TECHNOLOGY AND INFORMATION

**“SECURING CYBERSPACE: EFFORTS TO PROTECT NATIONAL
INFORMATION INFRASTRUCTURES CONTINUE TO FACE
CHALLENGES**

BEFORE THE

**SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION AND INTERNATIONAL SECURITY
OF THE SENATE COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENT AFFAIRS**

JULY 19, 2005
562 DIRKSEN BUILDING

Thank you for inviting me to appear before you today. I appear in two capacities, first representing the great State of Delaware as Secretary of Delaware's Technology and Information (DTI) agency, and second as the current President of the National Association of State Chief Information Officers, or "NASCIO." NASCIO represents state chief information officers and information resource executives and managers from the 50 states, six U.S. territories, and the District of Columbia. In most cases, the state CIO is appointed to his or her position by the governor.

First, I would like to say a special thank you to Delaware's Senator Tom Carper and his staff members for suggesting that DTI could contribute a state perspective on the issue of cybersecurity and the importance of protecting states' networks and information. As the State of Delaware's CIO in charge of all state government information and communications technology, one of my highest priorities is cybersecurity. When my fellow CIOs get together for NASCIO meetings, this is the one topic that is always at the top of our discussion list.

The security of Delaware's information technology system is critical to the well-being of our state as a whole, not just the business of the state, but its economy, the provision of federal services to our citizens and homeland security issues such as the protection and support of our first responders. Delaware is unique in that we have centralized the IT functionality across all levels of state government. This centralization helps us to more easily address and focus security efforts than in states where the IT functionality is more fragmented.

In the most simple of terms, keeping those who would wish to do us harm out of our network and systems is the primary challenge of IT security staff in Delaware and across the nation. This requires multiple layers of system protection and constant diligence. Delaware's state network may be small in comparison to some other states, yet we're responsible for over 130,000 users representing all three branches of government including our law enforcement and first responder communities. Additionally, we are responsible for the network welfare of Delaware's K through 12 students in 19 separate school districts, as well as two of our three public higher education institutions.

In 2004 we processed **84 million pieces** of inbound e-mail for state users. Of this, spam accounted for nearly 70% of all incoming mail, viruses accounted for 1.6 million messages and we logged over 100 thousand suspicious activity attempts, sometimes referred to as Trojan Horses. Starting this year, we've deployed new software that permits us to track network events on a daily basis and we estimate that we fend off nearly 3,000 daily attempts at entering our network. As you will see in the documentation that we have attached to the written version of my statement, these numbers are not out of line with what other states are seeing.

As we continue to implement new and better anti-spam and anti-spyware technology, we have seen these numbers drop significantly; yet, last month, (June 2005) our suspicious activity category, —the most dangerous type of all—**spiked from 7,000 attempts in May to 141,000 in June**. This sharp increase is attributable to the latest variant of a "worm" known as "mytopb".

Thankfully, because of our extreme diligence, we have not had a significant intrusion into our state network, however, just last month, one of Delaware's higher education facilities was the victim of an international "phishing" site, and our staff was called upon to make certain that their critical systems were not compromised.

"Keeping those that would wish to do us harm" out of our network requires multiple layers of protection and can make my agency unpopular with some of our users when we require them to remember a strong password, or limit their ability to access certain internet sites. While it is rarely a terrorist in the traditional sense of the word that threatens a state network, we do not focus specifically on who is trying to infiltrate our network. Rather, our goal is to keep all those with bad intentions from ever entering our system, whether they are in-state, in-country or an international friend sending us an e-mail message.

Without lapsing into too many technical terms, we deploy a number of different hardware and software products to protect our network. Some of the terms used have counterparts in the world of physical security—for example, firewalls keep unauthorized computer traffic out of our system, just as a firewall in an apartment building prevents fire from spreading. We use several intrusion detection and protection devices, just like a home security system detects an intruder when a window is opened and protects the residents by sounding an alarm. We even have "black lists" of computer sites that are known to cause problems.

We scan, scan, and scan again, all e-mail coming into the state network. We search for viruses, spam, and other recognized problems. In fact, we have developed working relationships with the FBI and others who perform vulnerability audits and scans for us. The IT arena is an environment where you cannot become complacent at any time. All users of the state network have their outbound connection to the Internet funneled through software programs that block problem websites based on their content along with known phishing sites. All downloads coming into our network are reviewed for viruses and spyware.

During times of heightened security alerts like that resulting from the recent terror incidents in London, we too raise the bar on cybersecurity. While we still practice all of the same system protections, we pay particular attention to the many alerts, notification and security bulletins. We increase our vigilance and our monitoring because we are well aware that a virus that begins in Asia can propagate to the U.S in a matter of a few short hours. In a very short period of time, it is possible for a system that has not been hardened or properly maintained to be completely overrun.

Delaware is the first state to be a part of Microsoft's Security Cooperation Program. This Security Cooperation program provides that Microsoft will issue early notification to us before the anticipated release of security bulletins, alerts and other critical information. We will share metric information with Microsoft regarding attempts into our system. We are also partners in the Multi-State Information Sharing and Analysis Center. During my tenure as CIO, we began an East Coast regional IT Roundtable that includes my peers from New Jersey, Pennsylvania, Maryland, Virginia, and the City of Philadelphia. As "neighbors" we share common borders and common vulnerabilities.

Protecting critical IT infrastructure does not come cheaply. We estimate that we spend \$5 million annually, or 15% of my annual budget on security. While we understand the necessity, these are state dollars that could be used for other projects to serve Delaware's citizens.

What does the future hold? Unfortunately I have to state that I believe that threats to cybersecurity will only increase and we will face continual attacks and attempts on multiple fronts. State IT officials must continually adjust how and what gets filtered, blocked or monitored. New threats appear almost daily and they can, in a matter of seconds, render services we've all come to depend upon like email and web browsing, completely unusable. In the worst case scenario, without proper protection and due diligence, an attack could potentially cripple or completely shut down an entire state government.

In the end, we all must understand that all critical infrastructure is the same by its very nature – critical - whether it is a roadway system or a data network. Infrastructure is all about moving people and information, and a state's network infrastructure is equally as important as its highways, electric power grid, or mass transit system.

Now, I will conclude my remarks with a few words about what NASCIO is doing in this area.

NASCIO applauds last Wednesday's announcement by Secretary Chertoff that he will create an assistant secretary for cybersecurity within the reorganized department. NASCIO has supported the calls for such a position and has endorsed past legislative efforts seeking to create the position. The state CIOs have also promoted this position during NASCIO's annual DC fly-ins, where they discuss state and federal IT issues with Congress, including this subcommittee. In fact, the state CIOs have made addressing deficiencies in public-sector cybersecurity the number one item on NASCIO's federal agenda. We believe that the creation of a higher-profile position for cybersecurity within DHS is an important symbolic statement to the nation as a whole. Now, we need to begin work in each of the critical sectors, including ours.

NASCIO has long seen the natural linkage between homeland security and the "state and local sector" CIOs, who oversee information and communications technologies that support the key public service. Section 7(c) of Homeland Security Presidential Directive (HSPD)-7 declares that: "It is the policy of the United States to enhance the protection of our Nation's critical infrastructure and key resources against terrorist acts that could...undermine State and local government capacities to maintain order and to deliver minimum essential public services." Section 15 designates "emergency services"—most of which are delivered by state and local authorities—as being among the nation's "critical infrastructure sectors."

The most disturbing thing that has been discovered by NASCIO's Information Security Committee is the fact that DHS has not included cybersecurity in the state and local planning and preparedness process. In 2003, DHS refined the national program for state-based domestic preparedness (originally developed in 1999) to better meet the realities of the terrorist threat to the United States. Thus, the State Domestic Preparedness Program was reborn as the State Homeland Security Assessment and Strategy (SHSAS) Program. Each State Administrative Agency (SAA)—the primary point of contact between DHS and state preparedness officials—was provided with a 194-page State Handbook, which provides an overview of the entire

strategy and assessment process, which is managed by DHS's Office for Domestic Preparedness (ODP).

A review of the handbook revealed that, while chemical, biological, radiological, nuclear, and explosive (CBRNE) WMD threats are addressed in detail, the "cyber" threats to state governments' critical information assets are not addressed at all. Thus, the participation of state CIOs in the DHS grant funding process was very uneven, ranging from high levels of involvement to no involvement at all.

Having provided you with this background, NASCIO comes prepared to offer the committee one substantive step that it can take toward improving intergovernmental cybersecurity. NASCIO has provided committee staff with language that encourages the Secretary to have Office of Domestic Preparedness (ODP) and NASCIO revise the existing strategy and assessment process to include a cybersecurity preparedness plan from each state CIO. That cybersecurity plan would be submitted to ODP by each state as part of the larger SHSAS process. We feel that closing this cybersecurity planning gap in the near term, and especially before the next round of grantmaking gets underway, is the single most important issue facing our sector today.

Finally, NASCIO wants to point out that information systems in general are the only part of the nation's critical infrastructure that is under attack everywhere, all the time—and these attacks are inflicting countless billions of dollars in damage. It is possible that cyber attacks—even those without terroristic intent—could disrupt governments' operations in general or homeland security mission-critical systems specifically. Therefore, it is our duty to secure these systems from all types of threats, regardless of the intent behind them and as soon as possible. As the CIO for the State of Delaware and as the President of NASCIO, I appreciate the work of the Subcommittee in confronting this national challenge.



COMMONWEALTH of VIRGINIA

Lemuel C. Stewart, Jr.
CIO of the Commonwealth
Email: lemu.stew.ar@vita.virginia.gov

VIRGINIA INFORMATION TECHNOLOGIES AGENCY
110 S. Seventh Street
Richmond, Virginia 23219
(804) 225-VITA (8482)

TDD VOICE -TEL. NO.
711

***VITA Security Incident Management
Program Information***

- VITA spent approximately \$150,000 in Fiscal Year 2005 to help the Commonwealth of Virginia prevent, respond to and recover from cyber attacks.
 - These expenditures enabled VITA to implement a basic statewide incident reporting and response capability as of January 1, 2005.
- Due to the marked increase in cyber attacks, and in order to implement a more full-featured program to safeguard the Commonwealth's data and information systems, VITA has budgeted \$1,500,000 for Fiscal Year 2006. This will enable a robust security incident reporting and response capability throughout the Commonwealth of Virginia's technology enterprise. This capability will automate incident reporting functions and will enable VITA to:
 - Coordinate sharing of information regarding cyber attacks among state agencies.
 - Analyze incidents and attacks based on information collected from throughout the Commonwealth's technology infrastructure.
 - Assess information security vulnerabilities throughout the Commonwealth.
 - Coordinate responses to incidents among state agencies.
 - Engage in forensic analysis of information security incidents.
- Budgeted funds will enable VITA to implement fundamental information security incident reporting and response capabilities. Additional future capabilities envisioned would enable VITA to:
 - Further automate incident identification and response processes at critical business system boundaries.
 - Extend these capabilities throughout the Commonwealth's technology infrastructure.
- Implementing additional capabilities will require significant additional funding.



COMMONWEALTH *of* VIRGINIA

Lemuel C. Stewart, Jr.
CIO of the Commonwealth
Email: lem.stewart@vita.virginia.gov

VIRGINIA INFORMATION TECHNOLOGIES AGENCY
110 S. Seventh Street
Richmond, Virginia 23219
(804) 225-VITA (8482)

TDD VOICE -TEL. NO.
711

***VITA Security Incident Management
Quick Facts***

- VITA spent approximately \$150,000 in Fiscal Year 2005 to help the Commonwealth of Virginia prevent, respond to and recover from cyber attacks.
- VITA has budgeted approximately \$1,500,000 for Fiscal Year 2006 to implement a more full-featured security incident reporting and response capability.
- VITA has received and responded to approximately four security incidents per month since implementation of an enterprise security incident reporting process in January of 2005.



**State of North Carolina
Office of Information Technology Services**

Michael F. Easley, Governor

George Bakolia, State Chief Information Officer

May 18, 2004

The Honorable Marc Basnight, Co-Chair
President Pro Tempore of the Senate
Joint Legislative Commission on Governmental Operations
2007 Legislative Building
Raleigh, NC 27601-2808

The Honorable James B. Black, Co-Chair
Speaker of the House of Representatives
Joint Legislative Commission on Governmental Operations
2304 Legislative Building
Raleigh, NC 27601-1096

The Honorable Richard T. Morgan, Co-Chair
Speaker of the House of Representatives
Joint Legislative Commission on Governmental Operations
301 Legislative Office Building
Raleigh, NC 27603-5925

RE: Executive Branch Information Security Assessment Required under G.S. §147-33.82(e1)

Dear Senator Basnight and Representatives Black and Morgan:

As State Chief Information Officer and as Secretary of the Information Resource Management Commission, I submit for your review a public report that summarizes the results of an information technology security assessment of executive branch agencies. Also enclosed with this letter is a chart that provides the overall information security rating for each agency that was assessed.

The enterprise-wide assessment is the result of the General Assembly mandate contained in G.S. §147-33.82(e1), which directed that the State Chief Information Officer assess the ability of each executive branch agency to comply with the current security enterprise-wide set of standards. The General Assembly also asked for current agency expenditures for information technology security, and an estimate of the cost of bringing all agencies into full compliance with the current standards.

Twenty-five agencies were assessed and provided with a detailed report that evaluates their information security strengths and weaknesses. These formal assessments include the rate of compliance with the standards in each agency and an assessment of each agency's security

Senator Marc Basnight
 Representative James B. Black
 Representative Richard T. Morgan
 May 18, 2004
 Page 2

organization, network security architecture, and current expenditures for information technology security. The assessments also estimate the cost to implement the security measures needed for each agency to fully comply with the standards. This public report summarizes the status of the assessment.

The effort expended by the staff of the North Carolina Office of Information Technology Services, industry experts selected to assist and the individual agencies to ensure a successful and thorough assessment was extraordinary. I commend all parties for working under extreme time constraints and for bringing the project in \$200,000 under the budgeted \$2 million. The assessment was truly a cooperative endeavor. I thank the agencies for their dedication of untold hours to provide the outside experts with the most complete information possible. I also wish to thank all of those outside participants who worked with us on the project: Gartner, Inc., which headed the Project Management Office and developed the assessment tool; and, the companies which performed the individual assessments – AlphaNumeric, Ciber, Cii, Ernst and Young, HCS, Pomeroy, Secure Enterprise, and Unisys.

The assessment results recommend a statewide approach to many information security initiatives, such as enterprise security awareness and training, improved risk management and business continuity plans. Gartner, Inc. recommends initial funding at a total of \$52.9 million, with \$38.8 million being used to replace outdated desktop operating systems throughout the executive branch, a move that will improve security of the state's network. Of the balance, funding is recommended to increase the levels of security staffing in agencies and to improve perimeter defenses on agency networks.

The assessment finding that an enterprise approach optimizes information technology security is consistent with the conclusions of two other legislatively mandated studies: a study of information technology expenditures in state government by the Office of State Budget and Management; and, the preliminary study of the state's legacy systems. The budget office study concluded that centralization of authority over the management of information technology inventory and procurement for enterprise, or common, programs can benefit the state significantly.

If I can provide you with any additional information, please let me know.

Sincerely,

George Bakolia

Enclosures

cc: Joint Legislative Commission on Governmental Operations
 Janet Smith, Acting IRMC Chair
 Ann Garrett, ITS Chief Information Security Officer
 Lynn Muchmore
 Mona Moon

Homeland Security Grant Projects
Michigan Department of Information Technology

Internet Filtering System (SurfControl): \$380,000

- System users will be prevented from accessing web sites that are deemed risks to the State's network and systems.
- Filtering and blocking will protect our organization from possible disclosure of confidential information, helps to ensure worker productivity by preventing access to sites that are not business related, and protects the network from valuable bandwidth diversion.
- Protection from malware infections (viruses, worms, Trojan programs, phishing scams, etc.) that may cause denial of government service to our citizens.
- Pilot executed Sept. 13 – Oct. 22: Showed surprising number of blocked connection attempts to access inappropriate sites: Gambling, Adult/Sexually Explicit, Chat, Tasteless & Offensive, Spyware sites, etc. (see IAP)

Anti-SPAM Filtering: \$180,000

- TrendMicro software resides on servers at the gateway and filters incoming spam to the State of Michigan resources. This same product is used at the gateway for the SOM's anti-virus solution so integration is well managed.
- Current percentage of inbound state SMTP mail that can be classified as SPAM with a high certainty: 25%
- Current percentage of inbound state SMTP mail that carry viruses: 32%
- Implementing the current version of Trend Micro's Virus and Spam will eliminate more than 30,000 messages per day

MPSCS Reliability & Interoperability: \$668,000 (SHSGP Funds) + \$75,000 (UASI Funds)

- This project acquires a transportable communications system that would be deployed in emergency situations that require enhanced radio coverage, interoperability with multiple law enforcement agencies, or if a remote tower was inoperable. The mobile system would provide extended coverage to an area involved in a special mobilization or other law enforcement event. It will be used to establish connectivity with the State of Michigan network through the MPSCS or other points of entry with the microwave capabilities

Generators for OPS & Treasury: \$840,000

- Large fixed generators for critical data centers used for Operations Center and Treasury data facilities to support critical SOM applications in case of power outage

Network Vulnerability Scanning: \$125,000

Security Awareness Web Portal: \$100,000

Network IDS for DMZ Resources: \$75,000

Event Correlation System: \$400,000

Hosting Center Firewalls: \$225,000

Internal Zone IDS: \$250,000

Network Analyzer: \$80,000

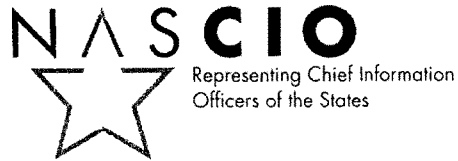
Incident Management: \$116,500

Network Penetration Study: \$178,000

GIS System for DIT Emergency Coordination Center: \$15,500

FARES Risk Analysis (Forensic Analysis of Risks in Enterprise Systems): \$100,000

VPN Proxy using SurfControl: \$25,000



KANSAS Quick Facts

Snapshot of Cybersecurity Expenditures FY 05, FY 06-08

FY 05

- ★ \$150,000 from network rate base for boundary control devices
- ★ \$ 250,000 for internal network security technology (ODP grant)
- ★ \$ 750,000 for critical infrastructure hardening (ODP grant)

FY 06-08

- ★ \$1,800,000 includes technology acquisition, FTE additions, training, penetration testing and audits. Amount to be supplemented by available grants

Over the past 18 months and using available technologies, Kansas has withstood 2 major intrusion attacks. During one of these attacks, boundary defense devices were processing and blocking 600,000 events per hour over a 3-4 hour time period. A third bot attack this spring produced minimal disruption on one network segment with an undetermined monetary cost.

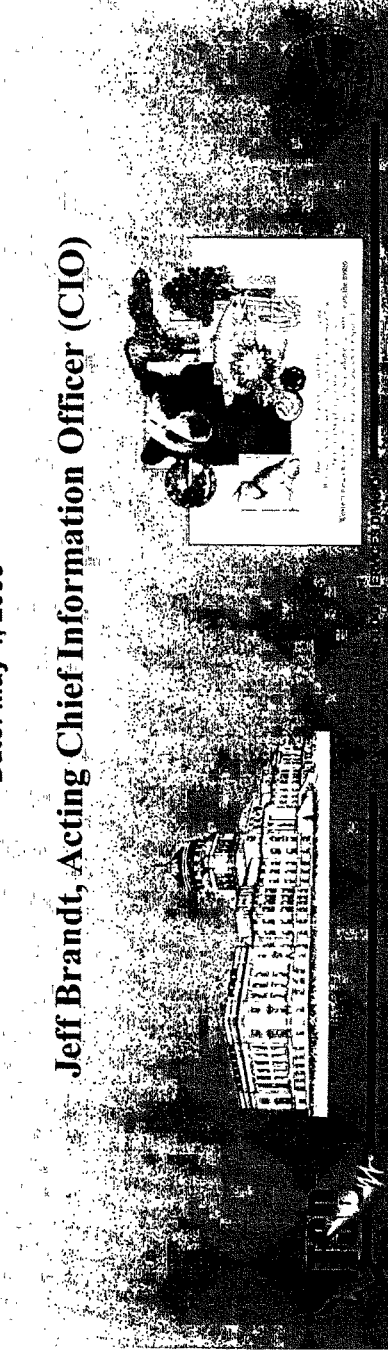
STATE OF MONTANA

Cyber Security Statistics

Presented to the Montana Congressional Delegation & the National
Association of State Chief Information Officers (NASCIO)

Date: May 4, 2005

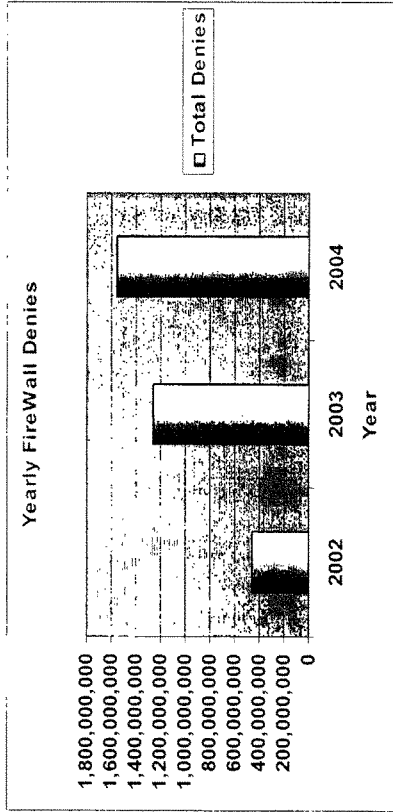
Jeff Brandt, Acting Chief Information Officer (CIO)



State of Montana - Intrusion Attempts

FIREWALL HITS REPORT 2002 TO CURRENT

Yearly access attempts DENIED by the Firewalls						
YEAR	TCP DENIES	UDP DENIES	ICMP DENIES	OTHER DENIES	TOTAL DENIES	TOTAL DENIES
2002	228,723,483	208,249,910	17,651,138	567,674	455,192,206	
2003	480,521,742	386,086,080	394,715,261	2,513,973	1,263,837,056	
2004	1,292,422,914	137,576,284	126,783,310	659,866	1,557,442,374	

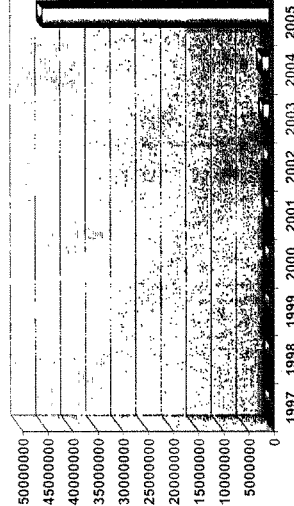


State of Montana – Virus Incidents (Attempted Infections)

STATE OF MONTANA YEARLY INCIDENT REPORT

Year	Virus Incidents
1997	93
1998	265
1999	2049
2000	6786
2001	53,358
2002	238,154
2003	1,148,434
2004	1,540,295
2005	45,323,902

Yearly Incident Graph

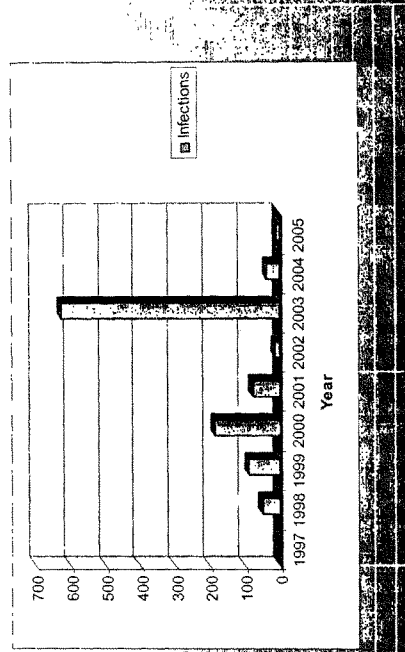


In 2005 we have added all Spam Totals from the State of Montana's Spam device. This device is stopping viruses as well as Spam.

State of Montana - Virus Infections

STATE OF MONTANA VIRUS INFECTIONS

Year	Virus Infections	Virus Examples
1997	0	
1998	48	
1999	89	Melissa
2000	184	ILoveYOU
2001	76	NIMDA, Code Red, KAK, SirCam, Magistr
2002	11	Klez, Bugbear
2003	625	Blaster, Nachi, Slammer, Sobig
2004	36	Blaster, Sasser, Netsky, Mydoom, Zaf
2005	8	Vundo, Troj/AgentSpy-B, Exploit-MIME.gen.exe



Questions and Responses from Mr. Purdy

Questions from Senator Coburn

Some have argued that the Interim National Infrastructure Protection Plan is vague regarding cyber security despite having a clear mandate by the Homeland Security Act of 2002 and later clarified by HSPD-7 for an integrated physical and cyber infrastructure protection plan.

When will the NIPP be completed?

Response: The NIPP Base Plan was released for comment on November 2nd. It includes enhancements in several areas, including the protection of cyber infrastructure. The revised Base Plan includes content throughout the document to address cyber security and the cross-sector cyber element of critical infrastructure and key resources protection across all 17 sectors. The NIPP also highlights cyber security concerns in an appendix that provides additional details on processes, procedures, and mechanisms needed to achieve NIPP goals and the supporting objectives for cyber security. The cyber appendix specifies cyber responsibilities for security partners, processes and initiatives to reduce cyber risk, and milestones and metrics to measure progress on enhancing the Nation's protection of cyber infrastructure.

This revised NIPP Base Plan, which addresses the Federal, State, territorial, tribal, local, and private sector roles and responsibilities for critical infrastructure protection, will be completed in early 2006. The 17 critical infrastructure and key resource (CI/KR) Sector-Specific Plans (SSPs) will further detail risk reduction strategies related to their respective critical cyber infrastructure.

Will the NIPP be beefed up with milestones which are linked to department heads and budget line items?

Response: The revised NIPP includes tables of key implementation actions that detail ongoing and future actions for the development and implementation of the overall national critical infrastructure protection program. These tables list activity milestones, timeframes for when they are to be achieved with respect to the date of final signature of the NIPP, and the responsible entity or entities (e.g., Department of Homeland Security, Sector-Specific Agencies [SSAs], security partners, etc.) for each activity milestone.

The revised NIPP Base Plan also has a chapter that describes the annual coordination process that DHS, the SSAs and other security partners will follow for resource allocation to address critical infrastructure and key resources protection. This chapter will also discuss the use of grant programs and regulatory and other funding authorities to maximize use of resources to support program priorities.

It seems that some industry sectors are more mature with regards to securing their cyber assets than others. It seems and as the title of the new Assistant Secretary for Cyber Security and Telecommunications would indicate that some critical infrastructures have more security needs than others, like the electric, chemical and telecommunications industry.

Which sectors are more technologically mature and could be used as examples for sectors that are less mature when building guidance with which to self regulate?

Response: Historically, some sectors such as the telecommunications, energy, information technology, and banking and finance sectors have led others in security best practices and in fostering awareness of cyber security overall. We are working to leverage these programs throughout other sectors.

Could you provide a sector-by-sector overview of the current status and the projected efforts of DHS information sharing activities with each of the critical infrastructures sectors within the next six months?

Response: DHS is currently focusing its information sharing efforts with the 17 CI/KR sectors on actions related to the completion and implementation of the NIPP and SSPs. The NIPP information-sharing strategy represents a fundamental change in how CI/KR security partners organize information and make decisions to prepare for, prevent, and respond to threats, incidents, and crises. This change constitutes a shift from information sharing and decision making among a small number of organizations, to a networked approach that affords the ability to move information both vertically and horizontally at great speed, and the ability to institute decentralized decision making. This networked approach will:

- Enable multi-directional information sharing between and across government and industry.
- Implement a common set of services — or baseline — of communication, coordination, and information sharing capabilities for all security partners.
- Provide all CI/KR sector owners and operators with a robust communications framework, tailored to the specific information sharing requirements, risk landscape, and protective architecture of each sector.
- Provide a comprehensive threat assessment picture to all security partners, including general and specific threats, incidents and events, impact assessments, and best practices.
- Maximize security partners' ability to assess risks, conduct risk management, invest in security measures, and allocate resources.
- Protect the integrity and sensitivity of shared information.

At the core of this networked approach is a series of sophisticated, secure tools and support mechanisms that facilitate rapid information sharing and coordination within and among

government and industry partners. This suite of tools, collectively referred to as the Homeland Security Information Network (HSIN), provides a national communications platform that enables the flow of near real-time information among governmental entities at all levels (i.e., Federal, State, territorial, local, and tribal), private sector organizations, and international security partners. By offering a user friendly, secure, and efficient conduit for the timely sharing of relevant information, the HSIN enhances the combined effectiveness of all security partners in preventing and responding to terrorist threats and attacks, and preparing for and responding to natural and man-made disasters.

Homeland Security Information Network

This web-based system provides participants direct access to an extensive suite of functions including mapping, robust search engine, instant messaging and chat (collaboration) and an information-posting capability which interfaces with both DOJ's Law Enforcement Online (LEO) and Regional Information Sharing System (RISS) networks. Within this framework, HSIN Critical Sector (HSIN-CS) is designed to enhance the protection, preparedness and crisis communication and coordination capabilities of the nation's 17 critical infrastructure and key resource sector owners and operators. HSIN-CS provides a mechanism for information sharing and collaboration within each sector, across the sectors, and between the sectors and the government. Some of the other key means of sharing information, which complement the HSIN, are described below.

➤ *Homeland Security Operations Center*

The Homeland Security Operations Center (HSOC) serves as the Nation's hub for information sharing, situational awareness, and domestic incident management—increasing coordination among Federal, State, Territorial, local, tribal, and private sector partners, as well as select members of the international community. The HSOC houses representatives from more than 35 agencies, ranging from State and local law enforcement to Federal intelligence agencies, each supporting and contributing to the vital information sharing and coordination functions of the center.

➤ *National Infrastructure Coordinating Center*

The National Infrastructure Coordinating Center (NICC) is a 24x7 watch operation center that maintains operational and situational awareness of the Nation's CI/KR sectors. As an extension of the HSOC, the NICC provides a centralized mechanism and process for information sharing and coordination between and among government, Sector Coordinating Councils, Government Coordinating Councils, and other private sector partners.

➤ *National Coordinating Center for Telecommunications*

The National Coordinating Center for Telecommunications (NCC) is a joint industry-government operation that regularly passes situational and operational information to the HSOC and other DHS components. The NCC coordinates with industry and Federal

Government organizations involved in responding to National Security/Emergency Preparedness (NS/EP) telecommunications service requirements.

NIPP Sector Partnership Model

The NIPP Sector Partnership Model encourages the formation of Sector Coordinating Councils and Government Coordinating Councils, and provides guidance, tools, and support so that these groups can work together and share information to enable all parties to carry out their protective functions.

➤ *Sector Coordinating Councils*

The Sector Partnership Model encourages owners and operators to create or identify a Sector Coordinating Council (SCC) as the government's principal point of entry into each sector for developing and coordinating a wide range of CI/KR protection activities and issues, including information sharing. SCCs are self-organized and self-governed, and are representative of owners and operators within a sector.

➤ *Government Coordinating Councils*

Complementary to the Sector Coordinating Council, a Government Coordinating Council (GCC) is formed as the government counterpart for each sector to enable inter-agency coordination. The GCC is composed of representatives from across various levels of government (Federal, State, Territorial, Local, and Tribal) as appropriate to the security landscape of each individual sector.

Information Sharing and Analysis Centers (ISACs)

The private sector has a number of established information-sharing mechanisms that contribute to the protection of their assets. One such mechanism is the ISAC. While the SCCs will consider the information-sharing needs of the private partners in each sector, ISACs and other existing mechanisms provide an array of options and capabilities for CI/KR owners and operators.

US-CERT Portal

Within NCSD, US-CERT utilizes a secure collaboration portal – the Homeland Security Information Network (HSIN)/US-CERT Portal – to share information with its partners. The portal contains a set of collaboration features to include secure messaging, libraries, forum discussions, alerts, chat rooms, calendars, online meetings, surveys, task tracking and a user locator. The portal is available to over 2,000 participants that represent Government, industry and the Information Sharing and Analysis Centers. With the launch of DHS's HSIN the US-CERT portal has been incorporated into the HSIN infrastructure as the cyber component. HSIN has developed dedicated portal space for several of the ISACs in its Critical Sector component (HSIN-CS). While the Information Technology ISAC (IT-ISAC) has its own portal, it has agreed that it will collaborate by incorporating its cyber information received from other sector ISACs into the US-CERT Portal and, therefore, into HSIN.

You testify that National Cyber Security Division is in the process of reviewing sector specific plans, training Sector Specific Agencies, and helping Sector Specific Plan authors with enhancing cyber aspects of their plans.

Which Sector specific plans has DHS received to date?

Response: In November 2004, DHS received and reviewed initial versions of the Sector Specific Plans (SSPs) from all 17 sectors. The next versions of the plans are due to DHS 180 days after the release of the Final NIPP Base Plan.

Are any of them in final draft?

Response: The plans submitted in 2004 were the first versions of the SSPs. The next versions are due 180 days after the release of the Final NIPP Base Plan.

How many are left to collect?

Response: All 17 plans were collected in November 2004, and the next versions are not due to DHS until 180 days after the release of the Final NIPP Base Plan.

GAO and others have pointed out that DHS efforts to promote a trusted (2) way communication and information sharing have been found lacking by the private sector and some federal agencies. In fact, your testimony reflects National Cyber Security Division's second priority is cyber risk management or assessing the threat and reducing the risk. However, you state "With regard to assessing the risk, NCSD collaborates with the law enforcement and the intelligence communities in a number of ways." This statement leads me to believe that the national cyber security division is taking a law enforcement perspective with regards to securing our critical infrastructures.

Do you envision the new Assistant Secretary for Cybersecurity and Telecommunications as fulfilling a role similar to the FBI's or as an impartial third party?

Response: Close coordination and interaction with law enforcement agencies that focus on cyber crime and other related efforts is an essential component of the national effort to secure cyberspace. The new Assistant Secretary will not possess law enforcement authority, but will need to continue to work closely with law enforcement agencies to understand threats and vulnerabilities posed by potentially criminal activities, and use that information to develop and

implement mitigation strategies. Under this new position, DHS will continue to enjoy the mutually supportive relationship with law enforcement it has established via the NCSD.

GAO recently reported that the National Cyber Security Division lacked sufficient organizational authority to serve as the “national focal point” for cyber security. Secretary Chertoff announced reorganization at the Department where he said he will be creating an Assistant Secretary for Cyber Security and Telecommunications to resolve the challenges related to a lack of authority.

Q02720: How will the new Assistant Secretary for Cyber Security and Telecommunications have the power to effectively resolve the difficulties the National Cyber Security Division was grappling with, specifically with regards to the following:

- Achieving organizational stability;
- Overcoming hiring and contracting issues;
- Increasing awareness about cyber security roles and capabilities;
- Establishing effective partnerships with stakeholders (other federal, state, and local governments and the private sector);
- Achieving two-way information sharing with these stakeholders;
- Providing and demonstrating the value of the new organization.

Response: Addressing organizational issues is central to Secretary Chertoff’s “Second Stage Review” (2SR) of the Department. The 2SR details a six-point agenda that includes improving DHS financial management, human resource development, procurement, and information technology, and realigning the DHS organization to maximize mission performance. Recognizing the importance of protecting critical cyber assets, Secretary Chertoff is increasing the authority for cyber security by placing the coordinated activities of the NCSD and NCS under an Assistant Secretary for Cyber Security and Telecommunications.

It has been clearly defined both in law, presidential directive and working documents that conflicts in cyberspace can have real consequences in the physical world. Digital Control Systems can be attacked to cause physical harm at chemical facilities, water facilities, pipelines, telecommunications and the electric grid.

What steps has DHS taken to ensure that US CERT has the early warning capabilities and technical knowledge to address attacks or exploitation of operational control systems and what money is currently dedicated to this effort in the DHS budget?

Response: NCSD established the US-CERT Control Systems Security Center (CSSC) in partnership with Idaho National Laboratory (INL) and other Department of Energy (DOE) National Laboratories¹ in August 2004. Through the use of Cooperative Research and

¹ Pacific Northwest, Los Alamos, Argonne, Sandia, and Savannah River

Development Agreements (CRADA's) and other mutually benefiting agreements, the CSSC also incorporates partners from control systems industry associations, universities, vendors, and industry experts. The CSSC mission is to reduce the risk of cyber attacks on control systems and provides facilities and expertise to support the reduction of risk in critical infrastructure. Our control systems activities support NCSD's overall efforts to address cyber security across critical infrastructure sectors over the long term, as well as the US-CERT's capability in the management, response, and handling of incidents and vulnerabilities, and mitigation of threat actions specific to critical control systems functions.

To support early warning capabilities for operational control systems, US-CERT CSSC performs attack methodology analysis that involves evaluation and documentation of "hacker trends." In addition, US-CERT is engaged in Einstein and Internet Health Services Programs, which provide information on network traffic that allows analysis to be performed to determine if any traffic is targeted at control systems.

To develop an effective early warning capability, the Federal Government needs to obtain information related to cyber attacks and vulnerabilities from owners and operators. Early warning capabilities from operational control systems are highly dependent on notifications from the private sector community. The US-CERT Control Systems Security Center (CSSC) is working with Federal Energy Regulatory Commission (FERC), North American Electric Reliability Council (NERC), Information Sharing and Analysis Centers (ISACs), Sector Specific Agencies, and control systems owners, operators, and vendors to share information.

The CSSC helps US-CERT respond to incidents and manage vulnerabilities related to control systems. A dedicated CSSC help desk telephone number has been established to provide an initial point of contact for control system assistance and support, and a CSSC limited access secure portal (<https://us-cert.esportals.net/>) has been established for information coordination and dissemination of cyber threat and vulnerability alerts. A web site is under development to share control systems security information with our cyber security partners and the control system community. The web site, which will be available in FY06, will also provide information, resources, and links for owners and operators to obtain information to effectively defend their control systems.

The CSSC is also developing a control systems incident management support tool to enhance US-CERT cyber threat notification efforts. It is designed for use when a new vulnerability is detected and will enable the identification of critical infrastructure at greatest risk to an identified threat, enhancing CSSC's ability to rapidly notify facilities at greatest risk. Owners and operators can then implement protective measures as appropriate to reduce risk.

The NCSD Strategic Initiatives Branch has oversight responsibilities for the Control Systems Security Program, with a 2005 budget of \$11,794,000. US-CERT Operations also supports

control systems activities via its Einstein and Internet Health Services Programs; both with a total 2005 budget of \$13,250,000.

Help desk centers for operational control systems can be located in foreign countries and are given access to operational control systems within the United States remotely. Given the remote access that is built into operational control systems and the ability of vendors to hold proprietary information abroad, how does DHS plan to assess the risks that result from these inherent vulnerabilities and their implications for the safety and security of the Nation's critical infrastructures?

Response: The US-CERT Control Systems Security Center (CSSC) is very concerned about the various access points in US critical infrastructure that result from remote access to systems through international partners or off-shore outsourced activities. The US-CERT CSSC recently began discussions with a major international company to analyze risk and identify the optimum control system security measures specifically needed to respond to the concerns expressed above. This is the first in a series of discussions the US-CERT CSSC will have with all major vendors of control systems.

You state "DHS is ... encouraging U.S. software developers to raise the bar on software quality and security."

How are you encouraging software developers? How long has this been a policy of DHS? Please submit to the Committee a list of all efforts underway that support this statement.

Response: NCSD's Software Assurance activities and initiatives directly support the President's goals for securing cyberspace, as articulated in Priority II of the *National Strategy to Secure Cyberspace*, dated February 2003. Consistent with HSPD-7, NCSD serves as a focal point for software assurance, as part of ensuring the security of cyberspace, and works closely with the private sector, academia, and other government agencies to improve software development processes that will lead to the production of better quality and more secure software in support of improved software assurance.

DHS is encouraging software developers through a number of activities:

- Publicizing that security has to be "built in" rather than "bolted on" through various mechanisms such as software assurance forums, working groups, standards bodies, journal publications, etc;
- Working with developers and standards organizations to provide guideline materials for "securing the software lifecycle";
- Leading the development of the Software Assurance Common Body of Knowledge, which will provide a framework for developing education and training curriculum in

software assurance in coordination with standards bodies, government agencies, industry, and academia; and

- Sponsoring efforts with the National Institute of Standards and Technology (NIST) of the Department of Commerce to better ensure that the tools exist to help developers and acquirers have more comprehensive development, testing, and evaluation tools relative to software quality and security.

You talk about the development of a repository of best practices in your testimony. What is the current status of your efforts? How detailed are the guiding documents?

Response: DHS is currently developing and collecting software assurance and software security information that will help software developers, architects, and security practitioners to create secure systems. The web-based repository was launched in October 2005 and is available to the user community. Even with deep technical content, a business case is required to convince industry to adopt secure software development best practices and to educate consumers on the need for software assurance. For example, guidance on coding practices and coding rules is quite detailed and includes code fragments. On the other hand, in many areas of the software life cycle, software assurance research is ongoing, so the guidance tends to be less prescriptive. From a software engineering viewpoint, materials on the business case for improved software assurance, how to identify and analyze requirements, approaches to measurement, and suitable life-cycle processes are fairly high level and less prescriptive because these areas remain under active research.

Further you discuss the development of a software assurance common body of knowledge for curriculum development. Which institutions is DHS working with? Please provide the Committee copies of printed materials.

Response: DHS is developing the Software Assurance Common Body of Knowledge; the first draft was released in October 2005. DHS is working with the following institutions on this initiative:

- James Madison University
- Georgia Tech
- Wayne State University
- Defense Acquisition University
- Air Force Institute of Technology
- University of Maryland
- University of Detroit Mercy
- University of California - Davis
- Naval Post Graduate School
- Johns Hopkins University

- National Defense University Information Resource Management College
- Kennesaw State University
- University of Nebraska - Omaha
- Carnegie Mellon University
- National Institute of Standards and Technology (NIST)
- Department of Defense (DOD)
- National Security Agency (NSA)
- IEEE Reliability Society and Computer Society

Where has DHS published notices of its upcoming Software Assurance Forum?

Response: Notice of upcoming Software Assurance Forums can be found on the US-CERT Web site. E-mail invitations have been sent to established contacts with encouragement to further distribute the invitation to other stakeholders.

What dollar amounts has DHS spent on promoting investment in applicable software assurance research and development? Is DHS promoting this to the Private Sector?

Response: DHS investment in software assurance is reflected in its funding of software security studies, process development and technology transition, as well as research programs through the Science and Technology (S&T) Directorate. The overall S&T budget for cyber security in FY2005 is \$17M. DHS collaborates with the Private Sector and promotes investments in software security research, process development, and technology transfer through mechanisms such as conferences, working groups, speeches, and publications.

Further, DHS S&T recently held its August 2005 Conference, "Engaging the Private Sector: Homeland Security R&D Directions and Opportunities", which provided an opportunity for more than 800 attendees to gain a better understanding of the research, development, testing, and evaluation (RDT&E) needs of the Department; potential business opportunities; and R&D being pursued under DHS S&T sponsorship. Participants met senior management from the S&T Directorate and heard briefings from the Cyber Security Portfolio Manager and the Cyber Security Program Manager from the Homeland Security Advanced Research Projects Agency (HSARPA).

You mention in your testimony the National Cyber Response Coordination Group and its work with DOD and DOJ. Specifically, you talk about the development of a concept of operations or CONOPS for national cyber incident response. Defense and government operations are named critical infrastructures and important sectors, however, they are not owned by the private sector. Setting that aside,

When was the CONOPS first conceived? How far beyond the conceptualization stage are your efforts with regards to your (4) points?

Response: The need for a CONOPS was first identified in March 2004. The first two components have been completed, but are not yet ready for release. These include:

1. Mapping the current capabilities of government agencies related to cyber defense relative to detection and recognition of cyber activity of concern, attribution, response and mitigation, and reconstitution;
2. Identifying capabilities within the government that US-CERT should leverage to maximize interagency coordination of cyber defense capabilities:

The second two planned components include:

3. Performing a gap analysis to identify the surge capabilities for possible leverage by or collaboration with the US-CERT for cyber defense issues in order to detect potentially damaging activity in cyberspace, to analyze exploits and warn potential victims, to coordinate incident responses, and to restore essential services that have been damaged; and
4. Consider establishing formal resource sharing agreements with the other agencies per the cyber defense coordination needs identified through the process identified above.

Have efforts begun to map current agency capabilities?

Response: Yes, an original study of agency capabilities was conducted in the fall of 2003 and is being updated. The effort to update the agency capability mapping began in April 2005.

Who will be conducting mapping efforts?

Response: Through the interagency National Cyber Response Coordination Group (NCRCG), NCSD has been assigned to lead this effort.

Has a report been completed that identifies US-CERT capabilities?

Response: US CERT is part of the overall NCRCG agency capabilities mapping effort and has already been interviewed. Mapping of the current capabilities is complete, but the resulting documentation has not been completed.

What surge capabilities explicitly exist today and are in place?

Response: A myriad of different surge capabilities exist within the Federal Government. They range from computer forensic teams within law enforcement to computer code analysis teams, to situational awareness watch and warning elements. The GFIRST community of first responders is one source of surge capability. Another is the NCRCG that stands up during a cyber incident of national significance. Compiling this information is part of the overall agency capabilities mapping effort described.

Since 9/11, there has been talk about creating a reserve response team, has that been created and is that what you are proposing to create?

Response: The Department believes resources would be better used to support and leverage the existing response teams rather than creating new teams.

Finally, have formal resource sharing agreements been created and signed?

Response: In addition to the formal agreements that currently exist between DHS NCSD (as previously discussed) and other federal agencies such as NSA, Department of State, FBI and CIA, the NCSD Law Enforcement and Intelligence Branch is in the process of coordinating with the US States' Attorneys General to improve information sharing and collaboration efforts. Through these Memoranda of Agreement (MOAs) and non-disclosure agreements (NDAs), state, local, and tribal first responders will be selected and vetted to receive more timely threat information to enhance situational awareness and preparation, response, and recovery actions.

In your written testimony you focus heavily on DHS involvement with departments like DOD, DOJ, law enforcement, and intelligence communities. You do not focus heavily on your successes with the private sector. In standing with your testimony, you outline 2 overarching priorities. Specifically with regard to your first, Cyber Incident Management: A National Cyber Response System, you detail for the committee US-CERT's role in protecting and maintaining the continuity of our nation's cyber infrastructure.

Does US-CERT, beyond general warnings of virus etc..., represent a system that handles as well as encompass alerts, preparation, defense, response and recovery for operational control systems endemic in our Nation's critical infrastructures?

Response: Control systems are addressed by NCSD in a holistic manner and US-CERT is a component of this approach, handling readiness and response efforts for control systems as part of its larger effort. The preparation, defense, and recovery issues are also handled through the risk management framework of the NIPP. From an operations perspective, however, it may sometimes be difficult to determine if control systems have been compromised until there is a consequence due to the complex configuration of those control systems. In order to foster

greater awareness in this area, US-CERT is continuing to build relationships with the private sector to promote a trust-based environment for sharing information at the earliest possible stage for action. In partnership with DHS S&T, NCSD has established the Process Control Systems Forum to do that specifically with the control systems provider and user communities.

Specifically, you mention (4) major program activities, which program handles critical infrastructures?

Response: US-CERT's major program activities—(1) 24X7X365 cyber watch, warning, and incident response center, (2) malicious code analysis, (3) situational awareness, and (4) communication and collaboration among public agencies and key network defense service providers—are all designed to support the critical infrastructure protection efforts and are conducted in partnership with our private sector partners. Within NCSD, the Strategic Initiatives Branch manages activities to advance cyber security in critical infrastructure protection.

The CIP Cyber Security Program focuses on identifying and prioritizing cyber aspects of the nation's critical infrastructure/key resources. CIP Cyber Security has been delegated responsibility for carrying out the lead Sector Specific Agency (SSA) responsibilities related to the IT Sector. It is developing and implementing the IT Sector Specific Plan (SSP) through collaboration with the private sector to identify, prioritize, and coordinate the reduction of risk involving cyber assets. CIP Cyber Security is also working with other SSAs to ensure that cyber is considered across all of the critical infrastructure sectors. In addition, CIP Cyber Security is developing cyber guidance that will be shared with SSAs as they work to develop and revise their respective SSPs.

National Cyber Security Division established the US-CERT Control Systems Center.

When did the incident response facility at Idaho National Laboratories become operational?

Response: The US-CERT Control Systems Security Center (CSSC) instituted initial incident response capabilities at the Idaho National Lab (INL) in August 2004. Through partnerships with other National Laboratories, control systems vendors, and the private sector; and the development of technological improvements for systems and facilities, the US-CERT CSSC has been maturing their response abilities to support US-CERT with control system expertise. CSSC also has capabilities at INL to perform vulnerability assessments of control systems.

It is part of DOE's facility at INL?

Response: The assessment center is housed within the Department of Energy's (DOE) Information Operation & Research Center (IORC) facility. Both DOE and DHS have invested in enhancing the capability of the facility and share physical and subject matter expert resources.

Is there an alert system in place and active currently?

Response: The US-CERT support function at CSSC in Idaho is on 24/7 alert to respond to incoming requests from the US-CERT on matters relating to cyber attacks against control systems.

You point out as an accomplishment that NCSD has established relationships with more than 25 potential industry partners. How many agreements have been completed? Please give examples of how industry has benefited from this agreement.

Response: Partnerships with members of the control system community are designed to help NCSD better assist industry with critical infrastructure protection measures. Agreements with our private industry partners provide CSSC with access to subject matter expertise and the ability to perform specific tasks that promote and enhance the security of control systems.

Control system owners and associations provide operating experience, expertise, and insight into cyber security at their individual facilities, providing valuable assistance in NCSD's work to understand and resolve vulnerabilities in next generation and legacy systems. The following associations have participated in, or are currently planning, agreements to share information with CSSC:

- American Petroleum Institute
- Chemical Industry Data Exchange
- The Instrumentation, Systems, and Automation Society
- Railway Electronics Task Force and Association of American Railroads
- Water Environment Research Foundation

This public-private collaboration has benefited industry in numerous ways:

- Serves to focus attention on the control system vulnerabilities and the need for preparedness and reaction resolution.
- Serves to bring industry and government together to consolidate and devote efforts to finding solutions.
- Returns specific vulnerability data to vendors for their efforts in developing solutions within their product lines.
- Initiates the process of building the business case for change and raising the awareness of the need for security to ensure reliability of the systems in place.

You mention the creation of a Gross Consequences Matrix and a National Asset Database. Please work with my staff to organize a classified briefing to discuss the details of both the Matrix and the Database.

You testify that a quantitative control system cyber risk/ decision analysis measurement methodology has been created. Tell us about what it measures, factors, variables and have you proven it works?

Response: The CSSC Program supports the use of quantitative risk where both probability and consequence are estimated. Probability of occurrence is stated in terms of frequency (events per year being the preferred units), which is determined by a complex relationship between threat (both threat actors and threat vectors) and vulnerability (including the competition between system weaknesses and system defenses).

The difficulty of immediately applying quantitative risk analysis to the cyber control system security problem is the paucity of relevant input, including:

- Historical knowledge or frequency of cyber attacks on control systems;
- Current measurements of frequency of cyber attacks (categorized by threat actors and threat vectors) on control systems;
- System security strength;
- Attack scenarios on control systems;
- Value (positive) of security measures; and,
- Value (negative) of vulnerabilities.

CSSC risk analysis efforts related to development and use of this methodology include historical incident studies to determine historical attack frequency; cyber risk reduction estimation to demonstrate ability to measure risk reduction for an isolated system; critical infrastructure cyber consequence matrix application of the methodology to prioritize critical infrastructure facilities for cyber risk based on consequence; assessment templates to qualify system vulnerabilities; development of an integrated risk reduction tool (in progress); and, development and implementation of an incident management support tool to prioritize facilities at-risk upon discovery of a new vulnerability.

What does it measure?

It measures risk, or risk reduction depending on the specific application, in quantitative terms if possible, and in qualitative terms when quantification is not possible.

What are the factors?

Factors begin with a risk equation in which risk is equal to probability times consequence. Probability can be developed in factors of threat and vulnerability. Threat must be developed into factors of threat actors, their intent and capabilities, and threat vectors, which include all

elements of physical and cyber attacks. Vulnerability is a complex function of the physical system, human factors, computer software, and hardware. Vulnerability is balanced by defense measures, which include engineered controls (e.g., encryption, firewalls, intrusion detection) and administrative controls (e.g., policies, procedures, training, audits).

What are the variables?

All of the above factors may be variables, depending on the system under consideration.

Have you proven it works?

Quantitative risk analysis has been proven effective in many industries. For the CSSC, quantitative risk analysis has been shown to work on carefully defined and delimited problems. It cannot be immediately applied to arbitrary cyber control systems for the reasons stated above (e.g., lack of security metrics, quantified threat) without first developing the data required. It has also been successfully applied to the Critical Infrastructure Cyber Control Matrix (risk quantified based on worst case consequences) and to an isolated control system (measured risk reduction).

Further, you list (5) milestones. You do not list projected dates of completion or anticipated budget priorities associated with each item. Will you provide for the Committee those two items? Moreover, what progress have you made toward actualizing these milestones?

Response: The table below shows progress made toward actualizing the five milestones and lists projected dates of completion.

Milestone	Actions	Projected Date of Completion
1. Develop a comprehensive set of control systems security assurance levels for owners and operators.	Issue Draft Control Systems Security Framework, Version 0.9, which defines security requirements and sets security assurance levels	Completed 01-July-05
	Issue Draft Framework, Version 1.0, which provides additional solution sets by assurance level	Completed Sept-05
	Populate Framework Requirements Matrix to detail recommendations for meeting assurance levels and issue Version 1.0	Completed Sept-05
2. Sponsor government / industry workshops to increase awareness among control systems owners and operators of potential cyber incident impacts and vulnerabilities	Hold 1st Industry Awareness Workshop (United Telecom Conference)	Completed Apr-05
	Hold 2nd Industry Awareness Workshop (British Columbia Institute of Technology)	Completed Aug-05
	Hold 1st Industry Editorial Group Meeting	Completed Feb-05
	Hold Industry Awareness Workshop (Invensys SCADA User Group)	Completed Sept-05
	Hold Industry Awareness Workshop (Emerson Exchange 2005)	Completed Oct-05

	Hold Industry Awareness Workshop (Siemens User Group)	Completed Oct-05
	Hold Industry Awareness Workshop (ABB User Group)	Completed Oct-05
3. Develop, populate, and validate control systems security scenario assessment tools to provide response teams a web-based application to assess impacts	Launch semi-automated Self-Assessment Tool	Nov-05
	Develop architecture discovery tool	Nov-05
4. Assess a minimum of three cores systems and provide solutions to vulnerabilities and recommendations to protect against cyber threats	Assess 1 st core system	Completed
	Assess 2 nd core system	Completed
	Assess 3 rd core system	Dec-05
	Use recommendations to develop best practices for control systems community	March-06
5. Develop the US-CERT CSSC web page for information exchange	Complete Conceptual Design of Web Page	In Progress
	Launch Operational Web Page	March-06

You testify that the National Cyber Security Division has been supportive of efforts related to internet protocol version 6 and OMB's efforts to migrate federal agencies to this new standard.

Do federal agencies currently have internet protocol version 6 devices already installed, unknowingly?

Response: While NCSD has been supportive of efforts related to IPv6, NCSD is mindful of the security concerns related to IPv6 implementation. Federal agencies may have IPv6 installed because it is often indirectly enabled by the installation of new hardware and software devices. Most current operating systems now support IPv6 by default. As a result, auto configuration and the subsequent tunneling of IPv6 traffic through Federal networks may be unknowingly introduced by such an installation.

As indicated in the testimony, NCSD has been supportive of the Department of Commerce's (DOC) efforts related to Internet Protocol version 6 (IPv6).² The NCSD funded the IPv6 Task Force co-chaired by National Institute of Standards and Technology (NIST) and National

² The IP is a technical standard that enables computers and other devices to communicate with each other over networks, many of which interconnect to form the Internet. The current generation of IP, version 4 (IPv4) has been in use for more than 20 years. Through the guiding efforts of the Internet Engineering Task Force (IETF), a new version of IP, version 6, has been developed. Advantages of IPv6 over IPv4 include availability of more Internet addresses and additional user features and applications.

Telecommunications and Information Administration (NTIA) in conducting an economic study of issues related to IPv6 deployment.

Will intrusion detection systems pick-up this new protocol?

Response: Some network based intrusion detection systems are capable of supporting IPv6 and must be configured to support the protocol. US-CERT has issued information and guidance to the federal government community about IPv6 and the security risks that may be presented by default implementations and perimeter detection issues. US-CERT has recommended the following actions in the short term: IPv6 controls should be first implemented at the edge filtering devices; determine if firewalls and IDS products support IPv6 and implement additional IPv6 security measures; determine IPv6 devices and disable if not necessary; disable IPv6 use of standard configurations and/or with configuration management tools. US-CERT provided additional more specific recommendations as well, which may be provided upon request.

For decades the Nation has had detailed plans and programs for maintaining and recovering essential phone systems in the event of a national emergency (war, terrorism, or natural disaster)

What progress has DHS made in developing recovery plans and reconstitution capabilities for the key mechanisms of the internet? What plans exists?

Response: As described in the testimony, US-CERT Operations provides incident response functions for the Federal Government and has developed a CONOPs for that response mechanism. NCSD created a Cyber Annex to the National Response Plan that provides a framework for responding to cyber incidents of national significance. As such, the Cyber Annex formalized the National Cyber Response Coordination Group (NCRCG) as the principal federal interagency mechanism to coordinate preparation for, and response to, cyber incidents of national significance. Each of these efforts addresses response and recovery issues.

To specifically address the internet, DHS has formed a strategic partnership, the Internet Disruption Working Group (IDWG), between NCSD, NCS, the U.S. Department of Treasury (Treasury) and the U.S. Department of Defense (DoD) to establish priorities and develop action plans for responding to Internet disruptions of national significance. The IDWG is planning a forum to discuss action plans with private industry related to responding to disruptions to the Internet that have the ability to affect national, homeland and the economic security of the nation. At the IDWG Forum, specific topics of discussion will include:

- (1) the infrastructure components that represent key points of vulnerability for the Internet, for example, components that if destroyed or disabled would cause disruption for either the Internet in general, a wide scale area, or specific sectors, such as energy;

- (2) the identification of sector leaders, such as Internet service providers and telecommunications and information technology vendors that can play a lead role in coordinated response to Internet disruptions of national significance; and
- (3) an analysis of the capabilities required by those organizations to effectively respond and the action steps required to ensure that reconstitution can occur in the near term.

The IDWG will build upon its industry relationships established through the US-CERT, the National Security Telecommunications Advisory Council, and the National Coordinating Center for Telecommunications, as well as industry relationships maintained by the DoD and the Treasury, to bring together the right experts to discuss these issues. Through interactions with industry representatives prior to the forum, the IDWG understands that part of the value DHS can provide in assisting response and reconstitution from Internet disruptions involves formalizing responder relationships and coordinating and sharing situational awareness analysis across the interdependent sectors.

Further progress is being gained through the exercising and testing of response and recovery plans, which NCSD is accomplishing through sponsorship of the National Cyber Exercise: Cyber Storm planned for February 2006. Drawing conclusions from the exercise, and implementing lessons learned, will be critical to developing a national Internet response capability.

What steps is DHS taking to develop an early warning system that could identify indications and warning of wide spread attacks? Has DHS continued to develop the Global Early Warning Information System or has it developed something new to replace it?

Response: NCSD/US-CERT has multiple initiatives that support our situational awareness capacity. There are two programs focused on situational awareness within the government. First is the Internet Health Service, which obtains information about network activity and attacks from various private sources and provides them to the federal agency incident response community. The second is the US-CERT Einstein Program, a pilot program to monitor network activity in the federal agencies. NCSD conducted an evaluation of the Global Early Warning Information System (GEWIS) to determine which components of GEWIS provided value. While the GEWIS program has been eliminated as a result of that evaluation, the valuable components have been incorporated into the Einstein Program and the Internet Health Services Program.

In addition, NCSD/US-CERT utilizes a secure collaboration portal – the Homeland Security Information Network (HSIN)/US-CERT Portal – to share information and build increased situational awareness with the private sector. The HSIN has developed dedicated portal space for several of the ISACs in its Critical Sector component (HSIN-CS). While the Information Technology ISAC (IT-ISAC) has its own portal, it has agreed that it will collaborate by

incorporating its cyber information received from other sector ISACs into the US-CERT Portal and, therefore, into HSIN. NCSD is working to enhance international situational awareness through collaborative efforts with key global partners.

Do we know the threshold at which a disruption of the internet would trigger the National Response Plan and has the federal government's role in the recovery efforts been clearly articulated?

Response: The Cyber Annex to the National Response Plan (NRP) is activated in response to a cyber-related Incident of National Significance. According to the plan, "a cyber-related Incident of National Significance may take many forms: an organized cyber attack, an uncontrolled exploit such as a virus or worm, a natural disaster with significant cyber consequences, or other incidents capable of causing extensive damage to critical infrastructure or key assets." As the definition in the NRP is necessarily broad, it is necessary for NCSD to work together with its government partners and private industry stakeholders to gain perspective on the thresholds that could lead to a cyber-related Incident of National Significance. The IDWG will discuss thresholds at the IDWG Forum. The focus of the discussion will be first determining what risk scenarios would require or benefit from industry and government coordination, such as scenarios that would cause a loss of service at the core (transport disruption) or edge (access disruption) that would severely impact services or users critical to U.S. economic, homeland or national security. From an analysis of the risk scenarios discussion, and response capabilities currently in place, the IDWG will develop qualitative and quantitative guidance for measuring whether an event constitutes a cyber-related Incident of National Significance.

In addition, the Cyber Incident Annex to the National Response Plan formalized the existence of the NCRCG. The NCRCG membership documented those triggers for a cyber incident of national significance in the Concept of Operations and are:

1. Cyber incident that may relate to or constitute a terrorist attack, terrorist threat, threat to national security, disaster, or other cyber emergency requiring Federal Government response;
2. Confirmed significant cyber incident directed at one or more national critical infrastructures;
3. Cyber incidents that impact or potentially impacts national security, national economic security, public health or safety; or public confidence and morale;
4. Discovery of an exploitable vulnerability in a widely used protocol;
5. Other complex or unusual circumstances related to a Cyber Incident that requires interagency coordination; or,
6. Any Cyber Incident briefed to the President.

The recovery/reconstitution function is also documented in the Concept of Operations but is awaiting results of the capabilities mapping program to provide the necessary information for formulating a comprehensive, interagency approach.

Can you provide the Subcommittee with either a private briefing or a written summary of the lessons learned from the various exercises (i.e., TOPOFF3) NCSD has participated in as they related to cyber security?

Response: DHS can provide the Subcommittee with a private briefing of the lessons learned from regional critical infrastructure exercises that were co-sponsored in 2004 with State and local governments and infrastructure owner/operators in the Pacific Northwest and Gulf Coast regions. While cyber security components were not specifically exercised during the full scale TOPOFF3 exercise, DHS did sponsor two Cyber Tabletop Exercises with the states of Connecticut and New Jersey prior to the full-scale TOPOFF3 exercise.

The National Cyber Security Division and the National Communications System have established the Internet Disruption Working Group.

Would you provide the Committee a demonstrable list of achievements or actions taken to date? Please provide written examples of work product.

Response: The IDWG is planning an IDWG Forum for November 2005. The focus of the IDWG Forum is to identify and detail actions that can be taken in the near term to enhance Internet resilience by leveraging efforts and applying them to current issues. The IDWG Forum will allow DHS to engage with its private sector stakeholders to discuss actions that can be taken to respond to and protect against Internet disruptions. The forum will involve two days of results-oriented discussion between a diverse set of experts from private industry, academia, government, and international communities. This forum will differ from similar efforts conducted in the past through its focus on near term and actionable strategies for improving Internet resiliency. A specific focus of the event will be to gather feedback on the most likely risk scenarios facing the Internet infrastructure today. Further emphasis will be placed on discussing needs and requirements for industry-government coordination during Internet disruptions of national significance.

Prior to the IDWG Forum in November, NCSD will complete its analysis of vulnerabilities and policy recommendations published to date on Internet disruptions. This information will be shared with participants at the forum. NCSD will also work with its stakeholders to prepare white papers for discussion at the forum in the following areas:

- Scope of disruption analysis

- Key Internet infrastructure components
- Risk scenarios
- Situational awareness strategies
- Near term protective actions
- Near term response: operational methods
- Near term response: surge capabilities
- Metrics and Authority

The IDWG has drafted several documents specifically for use in planning the IDWG Forum including invitations, save the date notices, briefing materials, and an overview of the Forum. In addition, the IDWG has reviewed and summarized recommendations from various efforts across government and the private sector concerning Internet vulnerabilities.

DHS has a dual statutory responsibility 1) It must support the federal civilian agencies in incident response and 2) perform the broad range of specific cyber functions called for in the Homeland Security Act of 2002

What has DHS done to ensure that it can accomplish both missions?

Response: US-CERT provides a national coordination center that links public and private response capabilities to facilitate information sharing across all infrastructure sectors and to help protect and maintain the continuity of our nation's cyber infrastructure. As described in testimony, US-CERT has four major programs of activity. First, US-CERT is DHS's 24x7x365 cyber watch, warning and incident response center which provides coordinated response to cyber incidents, a web portal for secure communications with private and public sector stakeholders, a daily report, a public website (<http://www.us-cert.gov/>), and a National Cyber Alert System, which provides timely, actionable information to the public on both technical and non-technical bases. US-CERT conducts malicious code analysis, provides malware technical support, and conducts cyber threat and vulnerability analysis. These programs support both missions.

With regard to the first area of responsibility to support federal civilian agencies in incident response, US-CERT retains the function of the previously existing Federal Computer Incident Response Center (FedCIRC) as the mandated center for federal agencies with FISMA obligation to report cyber incidents. For additional cyber security support to the federal civilian agencies, US-CERT manages a situational awareness program that includes the US-CERT Einstein Program for monitoring network activity in the federal agencies and an Internet Health and Status service for government agency computer security incident response teams. And, US-CERT manages federal and special programs for communication and collaboration among public agencies and key network defense service providers. A key federal coordination program was established by NCSD to facilitate interagency information sharing and cooperation for readiness and response efforts: Government Forum of Incident Response and Security Teams (GFIRST).

The GFIRST has increased information sharing horizontally across previously stove-piped organizations and improved the overall cyber preparedness of the U.S. Government.

NCSD is engaged in the development and implementation of the NIPP that will serve to address critical infrastructure protection in the seventeen identified critical infrastructure sectors and key resource sectors. HSPD-7 outlines Sector Specific Agencies (SSAs) for each of the critical infrastructure sectors, with DHS serving as the overall coordinator for the NIPP program. DHS is the SSA with NCSD as the lead for the Information Technology (IT) Sector and works with the IT-ISAC and the developing Information Technology Sector Coordination Council (IT-SCC) to support the NIPP's national CIP Risk Management Framework.

In addition to its responsibility to work with the IT Sector to identify critical assets, assess vulnerabilities, and determine protective measures, NCSD is ensuring that cyber is comprehensive throughout the NIPP by providing guidance to the other critical infrastructure sectors in identifying, assessing, and protecting their cyber assets and cyber components of physical assets. This guidance includes contributing cyber elements to the NIPP Base Plan, reviewing the cyber aspects of Sector Specific Plans (SSPs), and delivering cyber CIP training to SSAs and SSP authors to help them enhance the cyber aspects of their SSPs, all of which are underway in NCSD.

What is the status of the Virginia location of the US-CERT Operations Branch? What is its specific mission? What capabilities does it now possess? Does it replicate the Carnegie-Mellon University location? Is it fully staffed?

Response: US-CERT Operations is currently based in temporary space at the DHS Glebe Road facility while the permanent space in the same location is being built out and configured for security and technical requirements. The Glebe Road location houses US-CERT's analysis and technical teams. US-CERT also maintains two seats in the Homeland Security Operations Center (HSOC) for 24x7x365 incident response and to facilitate rapid response and coordination with HSOC Senior Watch Officers. US-CERT receives support from Carnegie Mellon University's (CMU) Computer Emergency Response Team (CERT/CC), specifically in the areas of analysis, vulnerability handling, and technical expertise. US-CERT's operations do not replicate CMU's location.

According the GAO report NCSD strategic plan establishes objectives for improving federal incident response to cyber attacks and improving capabilities for cyber intelligence analysis.

Please tell the Committee when the detailed operations plan for federal incident response will be ready?

Response: As described in the testimony, US-CERT Operations provides incident response functions and has developed a CONOPs for that response mechanism. DHS created a Cyber Annex to the National Response Plan that provides a framework for responding to cyber incidents of national significance. As such, the Cyber Annex formalized the National Cyber Response Coordination Group (NCRCG) as the principal federal interagency mechanism to coordinate preparation for, and response to, cyber incidents of national significance. In summary, the Concept of Operations for the NCRCG is:

1. Cyber incident that may relate to or constitute a terrorist attack, terrorist threat, threat to national security, disaster, or other cyber emergency requiring Federal Government response;
2. Confirmed significant cyber incident directed at one or more national critical infrastructures;
3. Cyber incidents that impact or potentially impacts national security, national economic security, public health or safety; or public confidence and morale;
4. Discovery of an exploitable vulnerability in a widely used protocol;
5. Other complex or unusual circumstances related to a Cyber Incident that requires interagency coordination; or,
6. Any Cyber Incident briefed to the President.

The recovery/reconstitution function is also documented in the Concept of Operations but is waiting for the results of the capabilities mapping program to provide the necessary information for formulating a comprehensive, interagency approach. To achieve the next level of granularity, the NCRCG is currently developing standard operating procedures, based on the Interagency Incident Management Group (IIMG) model, to speak to the various incidents the NCRCG may need to address.

A set of NCRCG Standard Operating Procedures is under development, which will provide some discussion of federal incident response. US-CERT will play a large role in that effort and each Department/Agency will have their own plans and procedures.

What resources have you dedicated to building a cyber intelligence capability?

Response: NCSD has a Law Enforcement/Intelligence Branch. Members of that Branch include detailees from USSS and NSA. ICE, FBI, and CIA have provided part time personnel to act as liaisons between DHS and their agencies. There are MOUs currently being finalized for a full time FBI liaison and a part time State Department detailee. The branch has a full time individual assigned to the cyber cell at DHS' Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). The branch serves as the centralized repository/coordinator for cyber intelligence information between the US-CERT, Law Enforcement, the Intelligence Community and private sector partners.

Will the finalized NIPP include cyber intelligence capability, if so will it have milestones and a budget line item associated with it?

Response: The interim NIPP does not contain that provision currently. Therefore, there are no milestones or budget allocations. As with the National response Plan, there will be a Cyber Annex to the NIPP. It is intended that the final NIPP will include cyber threat analysis as part of the risk assessment process.

Questions from Senator Carper

The Government Accountability Office pointed out that there's a crisis of confidence in the Department of Homeland Security's National Cyber Security Division.

How can an Assistant Secretary for Cyber-security and telecommunications within the Department provide more confidence for the Department?

Response: The creation of a position for Assistant Secretary for Cyber Security and Telecommunications within the Department would elevate the position of cyber security in the Department and by doing so raise visibility for the issue. With the dissolution of the Critical Infrastructure Protection Board (CIPB) in the White House and the creation of DHS, the private sector called for a senior level position for cyber security in the Department. There have been renewed calls for elevating the position of cyber security to the Assistant Secretary level and this action further reflects the department's commitment to cyber security, while addressing stakeholder concerns.

Irrespective of the creation of this new position, NCSD continues to move forward with its existing programs and activities. Progress in these areas as well as continued outreach and engagement with its stakeholder community will further help to build confidence in the capabilities of the Division and the value of the ongoing work.

In the coming year, how will the Department foster stronger cyber security partnerships within the private sector?

Response: NCSD has sought and continues to seek ways to establish cyber security partnerships with the private sector. In order for DHS to be successful in protecting cyberspace and America's cyber assets, NCSD relies on such partnerships. In the coming year, NCSD plans to build on existing relationships in a number of areas to foster stronger partnerships with the private sector.

The pending structure of the National Infrastructure Protection Plan (NIPP) provides a framework for a more robust partnership with the private sector. This includes interaction with both the Information Technology sector, for which DHS is the Sector Specific Agency with NCSD as the lead, through work with the Information Technology Information Sharing and Analysis Center (IT-ISAC) and the Information Technology Sector Coordination Council (IT-SCC). It also includes the other critical infrastructure sectors for which NCSD provides cyber guidance. As the NIPP framework evolves, NCSD expects the relationships with the IT and other sectors to evolve as well. In addition to NCSD's collaboration with the IT Sector and other critical infrastructure sectors, three other components of NCSD's approach to reducing vulnerabilities entail collaboration with the private sector: the Internet Disruption Working Group (IDWG), the Control Systems Security Program, and the Software Assurance Program.

In addition to ongoing activities, NCSD has planned a number of new initiatives that will serve to foster stronger cyber security partnerships with the private sector. NCSD/US-CERT has planned two workshops with private sector incident response teams in September (one on the west coast and one on the east coast) to share information on structure and programs, incident response, and to seek ways for the government and industry to work together operationally. The stakeholders include computer security incident response teams (CSIRTs), Information Sharing and Analysis Centers (ISACs), managed security service providers (MSSPs), information technology vendors, security product and service providers, and other organizations that participate in cyber watch, warning, and response functions. Specifically, the workshops seek to: provide an understanding of US-CERT goals, accomplishments, and current activities; provide an understanding of how US-CERT works with its current set of collaborators; determine how US-CERT can best interact with US-based incident response teams; and identify specific next participants will take to move the collaboration forward. This effort follows the model NCSD/US-CERT has created with government agencies in the Government Forum of Incident Response Teams, or GFIRST, where operational teams establish working relationships and share information with their counterparts in other agencies.

Following on to two private sector meetings convened by Assistant Secretary for Infrastructure Protection Bob Stephan in July, as well as previous NCSD briefings with the stakeholder industry groups in spring 2005, NCSD is continuing to develop partnerships with private sector stakeholders. As a result of those meetings, NCSD has identified three areas for partnership with the private sector: Preparedness/Response, Information Sharing, and Recovery. Efforts to pursue work in these areas is underway, including identifying areas for immediate action such as determining likely attack/threat scenarios and information needed to improve situational awareness. In addition, NCSD and other government partners are actively participating in the Cyber Security Private Sector Retreat held by the National Cyber Security Partnership (a coalition of interested industry associations that formed out of the December 2003 Cyber Security Summit) on September 21-23, 2005. Areas of focus for that meeting include (1) information sharing; (2) roles, responsibilities, and recovery efforts between the government and private sector; and (3) incentives.

The Department of Homeland Security is actively involved with the Office of Management and Budget's Cyber-security Task Force to provide cyber-security technical expertise and recommendations to various Federal agencies.

Can you please describe this initiative, as well as any additional initiatives that the Department has in place to improve cyber-security within the Federal government?

Response: In March 2005, the Office of Management and Budget (OMB) created an inter-agency task force for the purpose of establishing an information systems security line of business (ISS LoB). The intent of the ISS LoB initiative is to establish common solutions and target architectures to increase operational efficiency and reduce resource requirements.

Presently, each agency individually develops, funds, and maintains many common security functions. Last year, the Federal government spent over \$4 billion securing its information technology infrastructure. Early analysis estimates that a significant portion of these resources were spent on implementing and maintaining duplicative and common processes. The ISS LoB initiative will recommend strategies for identifying and implementing standardized processes, products and services, improve security consistency and performance, and reduce overall costs. This will enable agencies to direct limited resources toward security quality instead of investing in the development of security processes.

Goals and objectives of the ISS LoB include:

1. Define and manage the Federal Government information security risk profiles
 - Define and establish consistent and measurable information security processes and controls across government
 - Identify problems and propose solutions that strengthen the ability of all agencies to defend against threats, correct vulnerabilities, and manage information security risks
2. Support performance of the Federal Government's mission through improved information sharing
 - Promote seamless, secure information sharing
 - Promote collaboration among agencies -- move from a reactive to proactive paradigm
 - Achieve efficiencies and effectiveness through standardization and sharing of capabilities, skills, and processes across government, where appropriate
3. Establish a mechanism to acquire, distribute and support information security solutions
 - Address emerging and unpredictable changes to budget and mission priorities
 - Improve and promote consistent security management processes and controls across government through adaptation of proven practices

- Achieve savings or cost avoidance through reduced duplication and economies of scale for common hardware, software and shared services
4. Leverage existing workforce resources capable of leading the confidentiality, integrity and availability of federal information and information systems and attract and retain supplemental workforce resources to this end
- Establish information security training baselines for users and role-based positions
 - Create a government-wide standard for information security competencies through an information systems security workforce roadmap (GoLearn)
 - Develop common criteria for credentialing information security professionals
 - Implement solutions for delivering training services

An integrated, Government-wide information systems security program could enable agencies' mission objectives through a comprehensive and consistently implemented set of risk-based, cost-effective controls and measures that adequately protect information contained in Federal government information systems. At the same time, there is not a "one size fits all" solution for information security for the Federal Government. Even though various information security requirements apply to every agency, there are some solutions that are mission specific and may not be suitable to all agencies. For example, a solution under the situational awareness and incident response activity area that works for some civilian agencies may not be appropriate for the intelligence community. The next steps for the line of business will be released with the President's budget in February.

In addition, DHS promotes and sponsors the development of guidance documents and tools that raise awareness and encourage the implementation of cyber security practices and processes across the Federal government. Activities include:

- Co-sponsoring the National Vulnerability Database (NVD), in conjunction with the National Institute of Standards and Technology (NIST), which is built on the Common Vulnerabilities and Exposure (CVE) standard and integrates all publicly available US Government vulnerability resources and provides links to industry resources;
- Improving the ability to standardize information across security advisories, tools, databases and services through promotion of expanded adoption of the CVE and open vulnerability and assessment language (OVAL) standards
- Sponsoring / developing cyber security guidance and best practices documents addressing malware, exercises, security configuration checklists, media destruction, and risk management; and,
- Sponsoring the creation of benchmarks for recommended security technical configurations.

In addition, NCSA/US-CERT has established a number of other initiatives to improve cyber security within the Federal government. These initiatives facilitate cyber situational awareness across the Federal government and specifically provide services to government agencies to

enhance their situational awareness. Further, these programs foster increased coordination and collaboration among Federal agencies.

The Internet Health Status Service facilitates federal agency detection of vulnerability, network attack, and malicious code activity by providing incident reporting and analysis from a variety of sources under agreement with US-CERT. This program is focused on tools and forensics and allows federal information security practitioners to utilize a resource for early warning alerts via the US-CERT Portal. US-CERT is also developing a tool that may be used by Federal agencies to determine whether they are affected by any known intrusion sets. US-CERT envisions that the program will be leveraged in the future to address emerging issues.

The Government Forum of Incident Response and Security Teams (GFIRST) was formed as one of two key federal coordination programs to facilitate interagency information sharing and cooperation for cyber readiness and response efforts. GFIRST is a group of technical and tactical practitioners of security response and are responsible for securing government information technology systems whose members work together to understand and handle computer security incidents and to encourage proactive and preventative security practices. The purpose of the GFIRST peer group is to: provide members with technical information, tools, methods, assistance, and guidance; coordinate proactive liaison activities and analytical support; further the development of quality products and services for the federal government; share specific technical details regarding incidents within a trusted U.S. Government environment on a peer-to-peer basis; and improve incident response operations.

GFIRST members consistently communicate with each other on the US-CERT Portal as well as meet on a regular basis. GFIRST held its first annual conference in April 2005 with over two hundred participants from Federal, State, and local governments. The conference was a major success for US-CERT and established further lines of communication. The technical workshops and speakers stimulated many technical interchanges regarding cyber first responder activities. GFIRST benefits from US-CERT's Internet Health Status Service.

Finally, GFIRST offers formal training to federal government employees via CERT/CC. The classes offered include: Technical Incident Handler Class, Advanced Technical Incident Handler Class; and, Managing a CSIRD.

The US-CERT Einstein program also enhances data sharing between Federal government agencies and the US-CERT, which provides an advanced cyber view and analysis of the Federal government's critical cyber networks. Einstein is currently deployed in the Departments of Treasury, Transportation, and Homeland Security, with five agencies to be added within the next six months. Einstein has an approved Privacy Impact Statement.

In your testimony, you state that the Department of Homeland Security will conduct a cyber-security preparedness and response exercise in November.

Who will participate in the exercise?

Response: The National Cyber Exercise: Cyber Storm will take place February 6-10, 2006. In the context of a cyber incident of national significance, the objective is to exercise: 1) the national cyber incident response community's policies; 2) information sharing mechanisms; and, 3) the community's procedures and processes for establishing situational awareness, supporting public and private sector decision making, communicating appropriate information to the public, and planning and implementing appropriate response and recovery activities. The exercise will involve representatives from across the Federal government, several international partners, and the private sector. Please find a detailed list of stakeholders and current participants below.

Cyber Storm Participants include:

- Department of Commerce
 - National Telecommunications & Information Administration (NTIA)
 - Bureau of Industry and Security
- Department of Defense
 - Office of the Assistant Secretary for Networks and Information Integration
 - Joint Staff
 - Northern Command
 - Strategic Command
 - Joint Force Component Command – Net Warfare
 - Joint Task Force – Global Network Operations
- Department of Energy
 - Office of Electricity Delivery and Energy Reliability
 - Chief Information Officer
- Department of Justice
 - Computer Crime and Intellectual Property Section
 - Federal Bureau of Investigation
- Department of State
 - Bureau of Diplomatic Security
 - Office of Critical Infrastructure Protection Policy
- Department of Transportation
 - Crisis Management Center
 - Federal Aviation Administration
- Department of Treasury
- Central Intelligence Agency
- National Security Agency
 - National Security Agency Threat Operations Center/ National Security Incident Response Center
- Office of Management & Budget
- National Security Council
- Homeland Security Council
- Interagency Groups

- National Cyber Response Coordination Group (NCRCG)
 - Interagency Incident Management Group (IIMG)
- Multi-State Information Sharing and Analysis Center (ISAC)
 - Select States
- Information Technology ISAC
 - Select Private Sector firms
- Communications ISAC
 - Private Sector representation (within exercise control cell)
- North American Electric Reliability Council
 - Electricity Sector ISAC
 - Select power industry firms
- Transportation Private Sector
 - NAVCAN (Canadian FAA)
 - FAA Network Service Provider
 - Select airline industry firms
- International Participants (Government leads listed below)
 - UK – National Infrastructure Security Co-Ordination Centre
 - Canada – Public Safety and Emergency Preparedness Canada
 - Australia – Attorney General's Office
 - New Zealand – Centre for Critical Infrastructure Protection
- Department of Homeland Security
 - NCS/US-CERT
 - NCS
 - Transportation Security Administration (TSA)/Transportation Security Operations Center (TSOC)
 - U.S. Secret Service (USSS)
 - Homeland Security Operations Center (HSOC)/Homeland Security Information Network (HSIN)
 - Protected Critical Infrastructure Information (PCII) Program Office
 - Infrastructure Coordination Division (ICD)
 - Office of Information Analysis (IA)
 - Protective Security Division (PSD)
 - Immigration and Customs Enforcement (ICE) (TBC)
 - Science and Technology (S&T) Directorate
 - I-Staff /Incident Management Division (IMD)
 - Office of Legislative Affairs
 - Office of Public Affairs
 - Office of General Counsel
 - Office of State and Local Government Coordination and Preparedness

How does the Department of Homeland Security plan to involve State agencies and officials?

Response: NCS/US-CERT is currently working with the Secretary's office to finalize the appropriate level of State involvement in the exercise. It is anticipated that 2-3 states will participate, primarily through their respective Offices of the Chief Information Officer / Chief Information Security Officer. DHS can provide additional details once the recommendations for State participation are finalized.

Questions from Senator Akaka

What efforts has DHS made to develop a strategic analysis and warning capability as recommended by GAO?

Response: A core component of NCSD and our effort to establish a National Cyberspace Response System is the US-CERT Operations Center. The overarching approach to this task is to facilitate and implement systemic global and domestic coordination of deterrence from, preparation for, defense against, response to, and recovery from cyber incidents and attacks across the United States, as well as from the cyber consequences of physical attacks or natural disasters.

US-CERT has four major programs of activity. First, US-CERT is DHS's 24x7x365 cyber watch, warning, and incident response center, and provides coordinated response to cyber incidents, a web portal for secure communications with private and public sector stakeholders, a daily report, a public website (<http://www.us-cert.gov/>), and a National Cyber Alert System, which provides timely, actionable information to the public on both technical and non-technical bases. We were integrally involved in efforts with private sector and government stakeholders to provide alert and mitigation information regarding the recent Cisco router and Microsoft Zotob worm incidents. After the initial alerts and advisories were issued with protective guidance against the Zotob worm and its variants, US-CERT engaged in a variety of efforts with stakeholder groups in the technical, vendor, Internet Service Provider, Federal Government, and control systems communities to gauge the impact and health of the public and private sectors. We continue to monitor and collect counts of infected machines and provide protective guidance as needed.

Second, US-CERT conducts malicious code analysis, provides malware technical support, and conducts cyber threat and vulnerability analysis. Third, US-CERT manages a situational awareness program that includes the Einstein Program for monitoring network activity in the federal agencies, currently operational at three agencies, with five pending deployments within the next four to six months; and an Internet Health and Status service used by 50 government agency computer security incident response teams. Fourth, US-CERT manages programs for communication and collaboration among public agencies and key network defense service providers. In line with NCSD's close working relationship with NCS, US-CERT works closely with the National Coordinating Center for Telecommunications (NCC) to address and mitigate cyber threats including response and recovery. U.S. CERT also maintains a presence in the HSOC to ensure coordination throughout DHS.

As you move forward with much-needed efforts to strengthen cyber-security, what must be done to ensure that the privacy rights of the American public are protected?

Response: The Department of Homeland Security is committed to protecting the privacy rights of all Americans in implementing programs to protect homeland security. DHS has its own statutorily-mandated Chief Privacy Officer whose responsibility ensures, among other duties, that technologies sustain, and do not erode, privacy protections. The National Cyber-Security Division of DHS has its own Privacy Officer, who works closely with the DHS Chief Privacy Officer, to ensure that privacy is considered throughout the development life-cycle for DHS programs.

While many courts have not found a protectible privacy interest in IP addresses, the Department considers such personally identifiable information as requiring privacy protection. Accordingly, to the extent that our cyber-security programs collect, use or maintain this kind of personally identifiable information, we ensure that privacy impact assessments are drafted early in the development of these programs. The assessments help us ensure that appropriate privacy policies are put in place.

According to a GAO report issued last Friday, 24 major federal agencies have weaknesses in their own information security systems. Ironically, the Department of Homeland Security – our nation’s lead agency on cyber-security – is one of those agencies. What is the National Cyber Security Division doing to ensure that the Department’s own networks are secure?

Response: NCSD is working towards being an example of FISMA compliance. In addition, NCSD works with the Chief Information Security Officer of the Department as well as with the Department’s Computer Security Incident Response Center (CSIRC) to share incident reporting and expertise within the Department as it does with other federal agencies.



G A O

Accountability • Integrity • Reliability

United States Government Accountability Office
Washington, DC 20548

August 26, 2005

The Honorable Tom Coburn, MD
Chairman, Subcommittee on Federal Financial
Management, Government Information,
and International Security
Committee on Homeland Security
and Governmental Affairs
United States Senate

Subject: *Critical Infrastructure Protection: Responses to Subcommittee Post-Hearing
Questions Concerning Challenges to Addressing Cybersecurity*

Dear Mr. Chairman:

This letter responds to your request that we answer questions relating to our testimony of July 19, 2005.¹ In that hearing, we discussed the status of the Department of Homeland Security's (DHS) efforts to fulfill its responsibilities to enhance the protection of computer systems that support the nation's critical infrastructures and to strengthen information security and related challenges. Your questions, along with our responses, follow.

1. Please characterize for us, how serious is the threat affecting our cyber resources?

With critical infrastructures' increasing reliance on computers and networks, more organizations and individuals can cause harm using cyber attacks. Government officials are increasingly concerned about attacks from individuals and groups with malicious intent—such as crime, terrorism, foreign intelligence gathering, and acts of war. For example, in February 2005, the Federal Bureau of Investigation Director testified that the cyber threat to the United States is serious.² The Director further stated that although individual hackers do not pose a great threat, hackers intent on stealing information or motivated by money are a concern—adding that “if this pool of talent is utilized by terrorists, foreign governments or criminal organizations, the potential for a successful cyber attack on our critical infrastructures is greatly increased.” In addition, experts agree that there has been a steady advance in the sophistication and effectiveness of attack technologies. Intruders quickly develop

¹GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity*, GAO-05-827T (Washington, D.C.: July 19, 2005).

²Testimony of Robert S. Mueller, III, Director, Federal Bureau of Investigation, before the Senate Select Committee on Intelligence (Feb. 16, 2005).

attacks to exploit vulnerabilities that have been discovered in products, use these attacks to compromise computers, and share them with other attackers. Further, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

2. *For several years, GAO has raised concerns about the lack of adequate analysis and warning capabilities for cyberspace security and infrastructure protection. Now that DHS has created US-CERT and formed various working groups to address the issue, what more needs to be done?*

Although DHS has made progress in providing analysis and warning capabilities, we recently reported that it had not yet developed or deployed a national indications and warning architecture for infrastructure protection, as called for in Homeland Security Presidential Directive 7, that would identify the precursors to a cyber attack.³ In addition, DHS officials acknowledged that the program's current analytical capabilities are not expected to provide national-level indicators and precursors to a cyber attack. DHS faces the same challenges in developing strategic analysis and warning capabilities that we reported on 4 years ago during a review of DHS's National Cyber Security Division's (NCSID) predecessor, the National Infrastructure Protection Center. In 2001, we reported that there was no generally accepted methodology for analyzing strategic cyber-based threats. Specifically, there was no standard terminology, no standard set of factors to consider, and no established thresholds for determining the sophistication of attack techniques. We also reported that the Center did not have the industry-specific data on factors such as critical systems components, known vulnerabilities, and interdependencies. We therefore recommended that the responsible executive-branch officials and agencies establish a capability for strategic analysis of computer-based threats, including developing a methodology, acquiring expertise, and obtaining infrastructure data. However, as we reported in May 2005, DHS officials had taken little action to establish this capability.⁴

3. *Does DHS currently possess documented policy, plans, and programs that would facilitate remediation of a widespread Internet outage resulting from a physical or cyber attack? If so, what role has the private sector played in developing the plans? If no plan exists, what are the impediments to developing such a plan?*

As we reported in May 2005, DHS did not yet have plans (or associated performance measures or milestones) for recovering key Internet functions, for testing federal continuity plans, or for providing technical assistance to both private-sector and other government entities as they develop their own emergency recovery plans.

³GAO, *Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities*, GAO-05-434 (Washington, D.C.: May 26, 2005).

⁴GAO-05-434

Without plans to address the recovery of key Internet functions, it is unclear how recovery would be performed and how federal capabilities could be used to assist with recovery.

To address the issue of recovering key Internet functions and coordinating cybersecurity contingency plans, DHS formed the Internet Disruption Working Group. Among other things, this group is to determine the operational dependency of critical infrastructure sectors on the Internet, assess the consequences of the loss of Internet functionality, and work with stakeholders to identify and prioritize short-term protective measures and reconstitution measures to be used in the event of a major disruption. The working group is composed of federal agencies with an interest in preventing a major interruption on the Internet. In addition, at the time of our May 2005 report, the working group was attempting to include key private-sector individuals, specifically from Internet companies, in its efforts. These individuals would also likely include telecommunications and energy sector representatives. In addition to the lack of plans in this area, another impediment is DHS's ability to develop effective public-private partnerships, which we have previously reported as a challenge for DHS. Specifically, we reported that DHS had not developed partnerships based on the principles of building relationships with mutually developed goals, shared benefits and responsibilities, and tangible, measurable results.

4. *DHS was formed to prevent, detect, and recover from terrorism. Currently, there are concerns that DHS's significant cyber responsibilities are not getting the attention they deserve because the department's primary focus is on physical attacks. Could a more senior position, such as an Assistant Secretary for Cyberspace Security and Telecommunications help resolve this challenge?*

On July 13, 2005, the Secretary of Homeland Security announced organizational adjustments to DHS that included the creation of a new Assistant Secretary for Cyber Security and Telecommunications to be responsible for identifying and assessing the vulnerability of critical telecommunications infrastructures and assets; providing timely, actionable and valuable threat information; and leading the national response to cyber and telecommunications attacks. The establishment of this new position could improve federal cyber-critical infrastructure protection efforts by stabilizing DHS's leadership and providing greater visibility and authority for DHS's cybersecurity responsibilities. However, the success of the new Assistant Secretary will depend upon his or her organization's ability to overcome the challenges we recently identified in our May 2005 report, including gaining organizational authority; increasing awareness about its cybersecurity roles and capabilities; establishing effective partnerships with stakeholders (other federal, state, and local governments and the private sector); achieving two-way information sharing with these stakeholders; and providing and demonstrating the value DHS can provide.

5. DHS in its response letter to GAO states that it does have a strategic plan with milestones and performance measures. Why is their list insufficient?

In our May 2005, we acknowledged DHS's strategic planning efforts; however, its strategic plans lacked details, milestones, and measures. At the national level, the Interim National Infrastructure Protection Plan, issued by DHS in February 2005, does not include detailed plans for addressing cybersecurity in the infrastructure sectors; is not yet final; and lacks required milestones. In addition, DHS's strategic plan for its cybersecurity efforts does not include specific initiatives that would ensure that the challenges, which we identified in our May 2005 report, are addressed in a prioritized and comprehensive manner. Further, this plan does not identify the relative priority of its initiatives and does not consistently identify performance measures for completing its initiatives. Therefore, we recommended in May 2005 that DHS identify performance measures and milestones for fulfilling its responsibilities and for performing activities to address its challenges. Further, we recommended that the Department track organizational progress against these measures and milestones.

6. DHS suggests it already provides a prioritized list of key activities that are reviewed, updated and revised regularly. Why is their list insufficient?

As we reported in May 2005, DHS's strategic plan for its cybersecurity efforts did not identify the relative priority of its initiatives and does not consistently identify performance measures for completing its initiatives. Therefore, we recommended that DHS engage appropriate stakeholders to prioritize key cybersecurity responsibilities so that the most important activities are addressed first and develop a prioritized list of key activities for addressing the underlying challenges that are impeding execution of its responsibilities.

7. Many cybersecurity requirements have been in place since the late 1990's. How do we position the nation to more effectively address them and better deal with cybersecurity threats and vulnerabilities?

In order to better position the nation to more effectively address cybersecurity requirements and better deal with cybersecurity threats and vulnerabilities, DHS must accomplish the 13 key responsibilities in a prioritized and comprehensive manner. In addition, DHS should address the challenges that we reported in our May 2005 report, including developing effective partnerships and improving two-way information sharing. As we recommended in May 2005, DHS should prioritize key cybersecurity responsibilities so that the most important activities are addressed first, including responsibilities such as (1) performing a national cyber threat assessment; (2) facilitating sector cyber vulnerability assessments—to include identification of cross-sector interdependencies; and (3) establishing contingency plans for cybersecurity, including recovery plans for key Internet functions.

8. *GAO has identified a "roadmap" of 13 key responsibilities DHS needs to deliver on. Where should they focus first?*

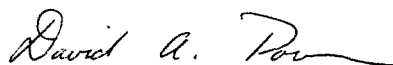
We recommended that DHS accomplish the 13 key responsibilities in a prioritized manner so that the most important activities are addressed first, such as vulnerability assessments and key recovery plans. In addition, DHS could focus initially on challenges that are more within their direct control such as completing a national threat assessment and raising awareness about DHS roles and capabilities. Further, the completion of National Infrastructure Protection Plan may also better position DHS to address its key responsibilities.

- - - - -

In responding to these questions, we relied on previously reported information and agency documentation describing DHS's responsibilities, and the status of its efforts that had been compiled in support of our May 2005 report and the July 19, 2005, testimony.⁵ We performed our work in accordance with generally accepted government auditing standards during August 2005.

Should you or your office have any questions on matters discussed in this letter, please contact me at (202) 512-9286 or pownerd@gao.gov.

Sincerely yours,



David A. Powner
Director, Information Technology
Management Issues

(310807)

⁵GAO-05-434 and GAO-05-827T

Questions and Responses from Mr. Skare for the Record

1. How many utilities when ordering new products are putting in their system specifications that they need security?

Most new RFPs in the US are now requiring security of some sort. The specification of security though is inconsistent and further, sometimes points to regulations like NERC 1300 which has been withdrawn and reissued as NERC CIP 2-9, or when specified as CIP 2-9 is unclear since CIP 2-9 are not approved and are changing (any business – vendor or Utility - is challenged to commit to open ended and changing requirements – Project Management 101). Siemens is committed to meeting the requirements when they are finalized and Siemens product cycles implement them. The specifics of what is required are not always specified. For example, specifying secure ICCP, DNP with AGA 12 security, etc, as opposed to saying ‘secure’.

2. What types of security are currently being put into place? Are there industry standards that are required or regulated?

Currently, support of NERC Urgent Action 1200 is in place, but this is a lowest common denominator approach. Secure ICCP has been implemented across our products lines, and general high level IT based security has been implemented to varying degrees. Since most SCADA systems are not procured with the network infrastructure, including routers, firewalls, Intrusion Detection Systems, etc, it is difficult for a vendor to know how a utility deploys the systems (which is a security issue for utilities, and wise of them to keep this information as secure as possible). Vendors (like Siemens) always recommend that the control systems networks are secured in this manner. Going forward, Siemens has plans in place for the next release of our products to add additional security features, as well as support for the current draft of NERC CIP 2-9. More advanced security features are also being defined for future releases after that. Draft Industry Standards such as IEC 62351 and AGA 12 must receive final approval. The temporary confusion created by the Energy Bill and the formation of an ERO by FERC must not slow the work on the NERC CIP 2-9 going to completion. More complete policy processes following ISO IEC 17799 targeted to electric sector control systems will also be of assistance. Finally, the lack of standardized interoperable security approaches with regards to key management in RTU

communications must be addressed (work that should be addressed in future AGA 12 work for example). The testing of AGA 12 at INL/PNNL/Sandia must be completed to judge effectiveness in the electric sector.

3. If a customer calls into the helpdesk with a locked out password is there a “back door” that the vendor can use to fix the problem? Have vendors of operational control systems built into their systems “back doors?”

No. All access methods to Siemens products are disclosed to customers so that there are no ‘back doors’. Customers are encouraged to change all base product passwords in delivered systems. All ‘locked out’ password situations would be handled by the customer themselves without involving Siemens. I am not aware of any password lockout situations or back door methods in our products.

4. Do vendors of SCADA systems regularly report SCADA breaches to the proper authorities? Of the breaches that do occur are they typically insider breaches or hacker type attacks? How many breaches has Siemens reported to law enforcement or related authorities world wide in the past 10 years?

Customers of SCADA systems generally do not report security breaches to their vendors. Utilities are very sensitive of having any security related information released. I am not aware of any reports from customers to Siemens, or from Siemens to law enforcement.

5. What type of encryption are customers of SCADA products or operational control systems using - internet language or communications language? If internet language, does that expose the systems dependant on communications language to any risks?

From an encryption perspective, there are not finalized and approved languages specific to Control Systems communications systems for the Electric Sector beyond what has been specified for Secure ICCP (IEC 60870-6). Work is underway with IEC 62351 and AGA 12, but the work is not

complete. Control Center to Control Center communications security (ICCP), was developed using IT methods and approaches (PKI) for this specific communications language. For RTU communications, the IEC 62351 is addressing IP based approaches, while AGA 12 is addressing Serial based approaches for now. Statistically speaking, no significant percentage of RTU communications are encrypted in the field today. The implementations that are in operation are generally not interoperable with other vendor's solutions.

However, encryption is not necessarily what is needed – the important thing to prevent a ‘man in the middle’ attack is Authentication, not Encryption. R&D is underway at PNNL on a new approach to hash communications with keys to Authenticate the communication without Encrypting it. Since the Electric Sector publicly posts operational plans for power per FERC orders 888/889 to make the Electric Market work, there is little to no consequence from viewing RTU communications – only undiscovered changes to the traffic (like from a Man in the Middle attack) can cause a consequence.

From a consequence point of view (the consequence of an attacker successfully performing a ‘man in the middle’ attack), serial RTU communications themselves are not an area of great concern as compared to IP based communications methods. Hacking into a serial line that is used for RTU communications does not provide additional access to a SCADA system or to an RTU. This means the worst case would typically involve sending false data back into SCADA, OR sending false commands down to the RTU OR more simply making the telemetry unavailable. This is isolated and limited in the effect that can be applied to the system as a whole.

This changes when IP based protocols are being discussed. These protocols (such as DNP over TCP/IP, or Modbus over TCP/IP) run over normal networking. Then, any vulnerabilities inherent in the network itself could be at stake beyond just the case of the serial protocols. Effectively, this means that the threats in the medium (serial line vs. network LAN/WAN) is

the source of more significant consequence than the protocols themselves.

6. What are you doing at Siemens' to protect customers? Do you use VPN to dial into customers systems when trouble shooting problems? What precautions do you use to protect back-up tapes of customers? Are back-up takes stored in foreign countries? Is Siemens typical of the industry?

Siemens is very active with our customers from an awareness and outreach perspective. Every User Group meeting has had topics of cyber security for almost a decade, and industry people have attended and given presentations as well (people such as Jeff Dagle from PNNL, and Scott Mix when he was with EPRI).

In addition, Siemens has implemented support for NERC 1200 in our control center products, and we have implemented SSL security for DNPI in our primary substation automation product in the US market (based on the CAISO RIG approach), and we have implemented Secure ICCP in all our control center products. Finally, our future product plans include securing both IP and Serial RTU communications as well as supporting the NERC CIP 2-9 requirements when they are finalized.

As a 'over the top' service, Siemens also offers an optional security service. This service (currently free for the asking for our customers who commit to a software subscription service) provides analysis of new security patches from third party vendors and recommendations on how to apply them to avoid conflicts with the operations of our systems. The recommendations are based on tests we perform after we determine the applicability of a patch to our system. While this may become required with future NERC CIP rules, Siemens has been gaining experience in this process since the beginning of 2003.

When remotely connecting to customers systems, Siemens usually uses a VPN connection controlled and turned on and off by the customer. It is generally specific to the one computer the customer has approved to remotely access their system under their control. In some cases, there could be a single modem for

access that is always unplugged unless the customer wants us to access the system, and then they plug it in for the duration of the support. These approaches are under the customer's control at their side. Siemens takes the security of these systems very seriously, and even has a process in place with Siemens Human Resources to notify our customers of any Siemens personnel with customer access that leave the company within 24 hours, in the spirit of following NERC rules.

Back-up tapes of customers in-house systems are protected by the project team and project manager on the Siemens side in partnership with the project manager and project team on the customer side. This is supported in accordance with the customer's wishes. These back-up tapes do NOT include operational data (Like live telemetry), but includes the source code and configuration data for the system. They are stored in-house or in a secure (US) off site storage facility if they get really old.

I suspect that Siemens is typical in this regard of the industry, with the exception of the security service which I believe is beyond what is typical.

7. In your testimony you talk about business process. What would motivate a company to make the investment into Cybersecurity to protect their critical infrastructures? How do you determine a return on investment after installing a security system and what are the risks?

This is really the 'Holy Grail' issue facing the industry today. Everyone wants secure solutions, but no one is willing to pay. Every security meeting in the industry mentions the need for business case support. But, due to the regulated nature of the Electric Sector with regard to rate structures, all investments must be approved by a rate case to each state's PUC. Utilities are loath to propose a new rate case for any reason that can avoid, because it is a lengthy, expensive process that sometimes reaches a decision in opposite of the goal of the Utility. As I understand it, this may have been impacted by the new Energy Bill, but from my perspective, it still appears that the Federal Government is not aligned or in synch with State Government.

To try and answer more directly the question, it always needs to be framed from the perspective of return on investment for the Utility. It is also possible, that by applying security to new technologies and methods of communications, cross over benefits may be realized. For example, by moving from outdated leased telephone lines to broadband IP based technology combined with a solid security solution, additional benefits such as accessing all the event and configuration data from all the substation IEDs becomes possible, in theory allowing the Utility to react to outages faster, thereby improving their service. Because reporting of security events is not done in the Electric Sector, there is a lack of evidence to point to that supports what the cost of a security event is. All that can be done is to look at the cost of recovering from a successful worm or virus attack, and extrapolate a reasonable comparison. The database of 60 or so events that has been collected by Eric Byers in British Columbia is reportedly the most complete collection of events in the process control industry. If a generic business case could be made based on that data and if the business case was posted on the PCSF, it could be used by everyone to promote securing of the systems.

As far as the methodology used to do the risk analysis, this is actually fairly well established by ISO/IEC 17799 and NIST SPP-ICS. But, they are not widely known yet, and they are onerous to perform. Basically, it means blueprinting the entire system, documenting all machines and connections, reviewing for vulnerabilities, performing some scanning to see what ports and services are open, and then once this is all done, consider for every vulnerability what the worst possible action that could be performed from the vulnerability, assess what this could mean in monetary value, assign a probability that this could happen, and in the end, dollars comes out. Then these dollars can be compared against the cost of fixing the vulnerabilities to determine the ROI.



STATE OF DELAWARE
DEPARTMENT OF TECHNOLOGY AND INFORMATION
801 SILVER LAKE BLVD.
DOVER, DELAWARE 19904

The Honorable Thomas M. Jarrett

Phone: (302) 739-9629
Fax: (302) 739-1442

To: Liz Scranton

From: Thomas Jarrett, Secretary

Date: 23 September 2005

RE: Responses to Congressional Testimony Questions

1. What procedures does the State of Delaware have in place to communicate with critical infrastructures sectors within its borders? Are there plans in place in the event of a cyber attack? How often is the State attacked? Were these plans developed with federal assistance? If so which agency (s)?

The State of Delaware is an active member of the Multi-State Information Sharing and Analysis Center (MS-ISAC) and we have adopted many of their guidelines for incident escalation and communication. We rely on our relationships with our peers in county and city governments, and private sector organizations to share critical data. DTT's response to a cyber attack will follow our established process for emergency activation and elevation. On October 13, DTI is hosting our first-ever cyber security tabletop exercise to practice our response and communication with others. More detailed planning for communication and response is forthcoming with the hiring of our first-ever Chief Security Officer position.

2. Does your office have regular contact with National Cyber Security Division at DHS? If not, which division do you have the most contact with?

No. During the monthly MS-ISAC teleconferences, Liesyl Franz, the Director of International Affairs and Public Policy and Deputy Director for Outreach and Awareness, frequently provides general updates to the states.

3. Does DHS proactively communicate with your office?

I receive the Daily Open Source Infrastructure Report from DHS, this is the only regular proactive communication.

4. What is the nature of the communication?

See answer 3. above

5. Have you ever received a cyber-security product from DHS? How often do you receive cyber-security products from DHS? Are these products informational, in response to a cyber incident, forecasting of upcoming issues of concern, etc.? Are these products helpful? How do you use the products you receive?

No, not aware of any cyber-security products that we've received from DHS.

6. Have you ever proactively provided information to DHS? What type of information and under what circumstances?

No.

7. Have you ever received funding or software/hardware from DHS? What have you done with the assistance you received?

We were the recipient of the ODP grant in FY04 and FY05 for patch management system, a visitor management system, client-server disaster recovery, and a cyber security awareness program.

8. How are you informed of a fast moving emerging cyber-security issue?

We are informed through a variety of sources--MS-ISAC, US-CERT, vendors, our peers in the private and public sector, and our internal monitoring tools.

NASCIO Responses

Q1: What type of information exchanges occur with other State CIOs and private industry?

A1: NASCIO assumes this question drives on two separate issues 1) Communications between the CIOs on cyber security and 2) exchanges between the CIOs and industry on cyber security.

1) NASCIO is not aware of significant CIO to CIO discussion or Coordination solely on cyber security issues beyond the strong focus provided by NASCIO. NASCIO has a standing Information Security Committee, which is led by state CIOs and is open to any state CIO or NASCIO corporate member with a particular interest in the issue. NASCIO also supports a listserv that includes the state chief information security officers (CISOs) of every state along with a few state CIOs. That listserv was used recently to convene a teleconference between the states and two corporate members who were involved in a minor security Controversy. Most discussions of cyber security operational issues and warnings occur among the members of the Multi-State ISAC (MS-ISAC), which also includes interfaces with industry.

2) NASCIO is aware that some states have separate relationships with

key IT/cyber security vendors who provide cyber security related information. NASCIO has recently increased its cooperation with some of these key vendors, but more is being done in this area. A number of states, through their Chief Information Security Officers, are participating with their local/state Infraguard chapters although the extent of that cooperation is unknown at this time.

Q2: Is DHS involved in this information exchange?

A2: NASCIO, as the association of the state CIOs, has had intermittent contact with DHS regarding cyber security issues, including discussions with former NCSD officials but has had no opportunities, despite making several outreaches, to work with DHS Office of State and Local/Government Coordination and Response. Other communications have been on a limited case by case basis. For example, NASCIO has responded to the occasional DHS solicitation for information--one notable example being after the Northeast Blackout.

Given that most information exchanges take place around alerting and other operational issues, they generally take place among the members of the MS-ISAC, where DHS alerting data such as that of US-CERT is forwarded to state members. A recent NASCIO cyber security related survey of states, conducted at the request of and in coordination with the House Homeland Security Committee staff, revealed that only 13 of 27 responding states had ever sought assistance from DHS on cyber-incidents. (We have no data on whether assistance was provided). Thus, NASCIO does not believe there is significant direct DHS - state CIO/CISO interaction on a national scale.